

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 07-295801

(43)Date of publication of application : 10.11.1995

(51)Int.Cl. G06F 9/06
G06F 12/14
G09C 1/00

(21)Application number : 07-090443

(71)Applicant : INTERNATL BUSINESS MACH
CORP <IBM>

(22)Date of filing : 17.04.1995

(72)Inventor : COOPER THOMAS E
PHILIPS HUDSON W
PRYOR ROBERT F

(30)Priority

Priority number : 94 235032 Priority date : 25.04.1994 Priority country : US

(54) DISTRIBUTION METHOD OF SOFTWARE OBJECT

(57)Abstract:

PURPOSE: To provide a method and device to distribute a software object from a source to a user.

CONSTITUTION: The software object is ciphered by a ciphering operation using a successive ciphering key.

The software object is sent from a source 209 to the user

211 and loaded to a data processing system for user control with a specific configuration. At least a computer

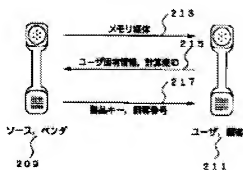
ID 215 consisting of a specific data processing system of the data processing system of user control is led out

from at least a part of the object. Furthermore, at least a temporary key 217 based on a successive ciphering key

and the computer ID 215 are led out from a part of the object. Since the successive key generating program is

served to receive the temporary key 217 to generate a

successive ciphering key, the user 211 uses the temporary key 217 for a prescribed period to access the software object thereby generating the successive ciphering key.



特開平7-295801

(43)公開日 平成7年(1995)11月10日

(51)Int.Cl. ⁵	識別記号	庁内整理番号	F I	技術表示箇所
G 0 6 F 9/06	5 5 0 C	7230-5B		
12/14	3 2 0 B			
	F			
G 0 9 C 1/00		9364-5L		

審査請求 未請求 請求項の数 8 O L (全 31 頁)

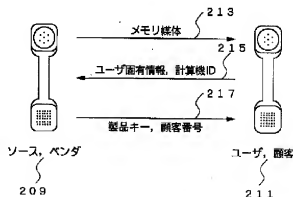
(21)出願番号	特願平7-90443	(71)出願人	390009531 インターナショナル・ビジネス・マシーンズ・コーポレーション INTERNATIONAL BUSINESS MACHINES CORPORATION アメリカ合衆国10504、ニューヨーク州アーモンク (番地なし)
(22)出願日	平成7年(1995)4月17日	(72)発明者	トーマス・イー・クーパー アメリカ合衆国80027 コロラド州ルイヴイル ウェスト・ウィロウ・ストリート 858
(31)優先権主張番号	2 3 5 0 3 2	(74)代理人	弁理士 合田 潔 (外2名)
(32)優先日	1994年4月25日		最終頁に続く
(33)優先権主張国	米国 (US)		

(54)【発明の名称】 ソフトウェア・オブジェクトの配布方法

(57)【要約】

【目的】 ソースからユーザにソフトウェア・オブジェクトを配布するための方法および装置を提供する。

【構成】 ソフトウェア・オブジェクトは永続暗号化キーを使用する暗号化操作で暗号化される。このソフトウェア・オブジェクトは、ソースからユーザに送られ、特定の構成を有するユーザ制御のデータ処理システムにロードされる。少なくとも一部がユーザ制御のデータ処理システムの特定のデータ処理システム構成に基づく計算機IDが導出される。また、少なくとも一部が計算機IDと永続暗号化キーに基づく一時キーが導出される。一時キーを受け取って、永続暗号化キーを生成するために永続キー生成プログラムが提供されるので、ユーザは、ソフトウェア・オブジェクトにアクセスするために、所定の期間、一時キーを使用して永続暗号化キーを生成することができる。



【特許請求の範囲】

【請求項1】供給側であるソースからユーザにソフトウェア・オブジェクトを配布する方法において、永続暗号化キーを使用する暗号化操作で前記ソフトウェア・オブジェクトを暗号化するステップと、前記ソースから前記ユーザに前記暗号化ソフトウェア・オブジェクトを送るステップと、

特定のシステム構成を有するユーザ制御のデータ処理システムに前記暗号化ソフトウェア・オブジェクトをロードするステップと、少なくとも一部が前記システム構成に基づく計算機IDを導出するステップと、

少なくとも一部が前記計算機IDと前記永続暗号化キーとに基づき一時キーを導出するステップと、所定の期間、前記ユーザが前記一時キーを使用して前記永続暗号化キーを生成できるように、前記一時キーを受け取って、前記永続暗号化キーを生成するための永続キー生成機能を動作させ、前記ソフトウェア・オブジェクトのアクセスを可能にするステップとを含む方法。

【請求項2】前記暗号化ソフトウェア・オブジェクトが、コンピュータがアクセス可能なメモリ媒体上に記録されて、前記ソースから前記ユーザに送られる、請求項1に記載のソフトウェア・オブジェクトを配布する方法。

【請求項3】前記永続キー生成機能が、前記コンピュータがアクセス可能なメモリ媒体上に保持され、前記暗号化ソフトウェア・オブジェクトとともに前記ソースから前記ユーザに送られる、請求項2に記載のソフトウェア・オブジェクトを配布する方法。

【請求項4】前記永続キー生成機能をその構成要素として含む、ファイル管理プログラムを、前記暗号化ソフトウェア・オブジェクトとともに前記ソースから前記ユーザに送るステップをさらに含む、請求項1に記載のソフトウェア・オブジェクトを配布する方法。

【請求項5】少なくとも前記一時キーを記録するために前記ユーザ制御のデータ処理システム内にキー・ファイルを作成するステップを含む、請求項1に記載のソフトウェア・オブジェクトを配布する方法。

【請求項6】少なくとも1つの固有のシステム属性を暗号化キーとして使用して、前記キー・ファイルを暗号化するステップを含む、請求項5に記載のソフトウェア・オブジェクトを配布する方法。

【請求項7】作成者からユーザにソフトウェア・オブジェクトを配布する方法において、永続キーを使用して前記ソフトウェア・オブジェクトを暗号化するステップと、

前記ソフトウェア・オブジェクトをコンピュータがアクセス可能なメモリ媒体にファイル管理プログラムとともに記録するステップと、

前記作成者から前記ユーザに前記コンピュータがアクセ

ス可能なメモリを送送するステップと、

前記ファイル管理プログラムをユーザ制御のデータ処理システムにロードし、それを前記ユーザ制御のデータ処理システム用のオペレーティング・システムに関連付けるステップと、

前記ファイル管理プログラムを使用して、前記ユーザ制御のデータ処理システムの少なくとも1つの属性に基づく計算機IDを導出するステップと、

前記ユーザ制御のデータ処理システムで前記コンピュータがアクセス可能なメモリを読み取るステップと、少なくとも一部が前記計算機IDに基づく一時キーを導出するステップと、

前記ユーザ制御のデータ処理システムで前記ファイル管理プログラムを実行することにより、前記一時キーによって定義される期間の間、前記ソフトウェア・オブジェクトへのアクセスを制限するステップと、

前記ユーザ制御のデータ処理システムにおいて永続キー生成機能を実行することにより、少なくとも前記一時キーを受け取ったことに対する応答として前記永続キーを提供するステップとを含む方法。

【請求項8】前記ファイル管理プログラムが、前記ユーザ制御のデータ処理システムによって実行されるときに、複数の動作モードで動作可能であり、(a)前記一時キーを使用することで前記ソフトウェア・オブジェクトが一時的に使用可能になる一時試用動作モードと、(b)前記ソフトウェア・オブジェクトを永続的に使用可能にして、前記ユーザによる前記ソフトウェア・オブジェクトの無制限使用を可能にする永続使用動作モードとを含むことを特徴とし、請求項7に記載のソフトウェア・オブジェクトを配布する方法。

【発明の詳細な説明】

【0001】

【産業上の利用分野】本発明は、一般的にはソフトウェア・オブジェクトへのアクセスを保護するための技法に関し、より具体的にはソフトウェア・オブジェクトへのアクセスを一時的に暗号化し制限するための技法に関する。

【0002】本発明は、“Method and Apparatus for Enabling Trial Period Use of Software Products: Method and Apparatus for Utilizing a Decryption Stub”という名称の米国特許出願第235033号、“Method and Apparatus for Enabling Trial Period Use of Software Products: Method and Apparatus for Allowing a Try-and-Buy User Interaction”という名称の米国特許出願第235035号、“Method and Apparatus for Enabling Trial Period Use of Software Products: Method and Apparatus for Utilizing an Encryption Header”という名称の米国特許出願第235031号、および“Method and Apparatus for Enabling Trial Period Use of Software Products: Method and Apparatus for

Allowing the Distribution of Software Objects”という名称の米国特許出願第 2 3 8 4 1 8 号に関連するものである。

【0003】

【従来の技術】ソフトウェア製品の作成と販売により、革新的な製品を有する企業に対して莫大な富が生み出されてきたが、時間が経つにつれて消費者がコンピュータに詳しくなるので、この傾向は今後も継続するものと考えられる。潜在的ユーザには市販されている様々な製品を走査検索する機会がほとんど与えられないため、コンピュータ・ソフトウェアは販売しにくいものである。通常、ソフトウェア製品はプラスチック・フィルムで収容包装された箱に収められており、潜在的顧客には、購入前に実際にそのソフトウェアを操作または体験する機会がほとんどまたはまったく与えられない。このため、消費者は、満足できるソフトウェア製品が見つかるまで複数の製品を次々に購入せざるを得ない場合が多く、製品に対する不満が募ってくる。これは、この世界で大量の海賊版ソフトウェアが発生している重大な原因の1つたり。潜在的ソフトウェア購入者は、ソフトウェアの一時使用という明白な意図を持って、友人や同僚から1組のディスクセットを「借りる」ことが多い。しかし、このような一時使用が長期間にわたり、潜在的顧客が実際にはソフトウェア製品を購入せず、借りたコピーに頼る可能性も多いだろう。

【0004】映画館には映画の予告編があり、テレビにはコマーシャルがあるが、ソフトウェア製品のサンプリングにはこのような共通の伝達経路が存在しないため、ソフトウェア・メーカは、新製品を宣伝し、新たな顧客を勧誘するために、印刷物やダイレクトメールによる宣伝に頼らざるを得ない。しかし、残念ながら、静的な印刷形式ではユーザと製品との対話をシミュレートすることができないため、印刷物は正確に製品を説明できない場合が多い。コンピュータ・ソフトウェア製品を購入するかどうか決心する前に顧客がその製品にアクセスでき、製品の違法使用する危険性を伴わずにこれを実現できるのであれば、ソフトウェア製品のメーカも顧客もどちらも十分要求が満たされるはずである。

【0005】暗号化したソフトウェア製品の配布は、購入前に潜在的ユーザに製品を配布するためにソフトウェア・ベンダが利用できる機構の1つであるが、製品へのユーザ・アクセスを可能にするキーを配布しなければならない。この場合、ベンダは、潜在的顧客の正直さと誠実さに完全に頼らざるを得ない。つまり、無節操な人や誠意のない人であれば、その友人や同僚にキーを渡し、無許可アクセスを可能にする恐れがある。さらに、無節操な人は、多数の人が無許可ユーザになれるように、一般の人がアクセス可能な掲示板にキーを掲載してしまう可能性もある。通常、このような安全保護違反は容易に防止することができないため、ベンダは潜在的顧客によ

る試用のためにソフトウェアを配布することを躊躇してきた。

【0006】

【発明が解決しようとする課題】本発明の目的は、一時的な試用期間を超えて海賊行為や無許可利用が行われるという不必要な危険性にソフトウェア製品を曝さずにユーザに一時的な試用期間を許可することと特徴とする、作成者から潜在的ユーザにソフトウェア・オブジェクトを配布するための方法および装置を提供することにある。

【0007】本発明の他の目的は、永続暗号化キー(long-lived encryption key)を使用してソフトウェア・オブジェクトが暗号化され、ソースからユーザに送られることを特徴とする、ソースからユーザにソフトウェア・オブジェクトを配布するための方法および装置を提供することにある。

【0008】本発明の他の目的は、コンピュータがアクセス可能なメモリ媒体に格納された特定のファイルへのアクセスを保護するための、データ処理システム内の方法および装置を提供することにある。

【0009】本発明の他の目的は、コンピュータがアクセス可能なメモリ媒体に格納された特定のファイルへのアクセスを保護するための、データ処理システム内の方法および装置を提供することにある。

【0010】本発明の他の目的は、ソースからユーザにソフトウェア・オブジェクトを配布するための方法および装置を提供することにある。この場合、コンピュータがアクセス可能なメモリ媒体がソースから潜在的ユーザに配布される。

【0011】

【課題を解決するための手段】本発明の第一の目的は、好ましくは、ソフトウェア・オブジェクトをファイル管理プログラムとともにコンピュータがアクセス可能なメモリ媒体で提供することと達成される。このソフトウェア・オブジェクトは、1つまたは複数の特定の暗号化操作により取消し可能な機能制限が施されていることが好ましい。コンピュータがアクセス可能なメモリ媒体は、従来の郵便および配送サービスを使用して作成者から潜在的ユーザに発送される。潜在的ユーザは、これを受け取ると、ユーザ制御のデータ処理システムにファイル管理プログラムをロードし、そのデータ処理システム用のオペレーティング・システムにそれを関連付ける。次に、ユーザ制御のデータ処理システムを使用してコンピュータがアクセス可能なメモリ媒体が読み取られる。ファイル管理プログラムは、ユーザ制御のデータ処理システムによって実行され、定義済みの一時試用期間の間、ソフトウェア・オブジェクトへのアクセスを制限するよう機能する。一時試用動作モードの間、ソフトウェア・オブジェクトの取消し可能機能制限を取り消すことで、ソフトウェア・オブジェクトが一時的に使用可能にな

る。これは、ユーザ制御のデータ処理システムのオペレーティング・システムがソフトウェア・オブジェクトを呼び出したときの暗号化ソフトウェア・オブジェクトの暗号解読によって達成されることが好ましい。ファイル管理プログラムは、オペレーティング・システムによって呼び出されたときに暗号化ソフトウェア・オブジェクトを一時的に解読するように、コピー操作を防止することが好ましい。潜在的ユーザがソフトウェア・オブジェクトの購入を選択した場合は、永続使用動作モードに入り、そこでソフトウェア・オブジェクトの機能制限が永続的に取り消され、潜在的ユーザがソフトウェア・オブジェクトを無制限に使用できるようになる。これにより、潜在的ユーザがソフトウェアを検討して、そのソフトウェアが自分のニーズに合っているかどうかを判定できるようにするためのブラウズ操作が容易になる。

【0012】ファイル管理プログラムは、ユーザ制御のデータ処理システムのオペレーティング・システムを連続監視し、システムの入力呼出しと出力呼出しを操作する。また、ファイル管理プログラムは、ユーザ制御のデータ処理システムのオペレーティング・システムが試用期間中にブラウズの対象となるソフトウェア・オブジェクトを要求した時点を識別する。その後、ファイル管理システムは、そのソフトウェア・オブジェクトに関連する一時アクセス・キーを取り出し、その一時アクセス・キーを検査して有効かどうかを判定する。次に、ファイル管理プログラムは、ソフトウェア・オブジェクトの機能制限を取り消し、処理のためにそれをデータ処理システムに渡す。

【0013】暗号化したソフトウェア・オブジェクトは、特定のシステム構成を有するユーザ制御のデータ処理システムにロードされる。その後、少なくとも一部がユーザ制御のデータ処理システムの特定の構成に基づく数値計算機ID (numerical machine identification) が導出される。次に、少なくとも一部がこの数値計算機IDと永続暗号化キーに基づく一時キーが導出される。この一時キーを受け取って永続暗号化キーを生成するための永続キー生成プログラムが提供されている。この一時キーを使用すると、ユーザはソフトウェア・オブジェクトにアクセスするための永続暗号化キーを所定の期間、生成することができる。これらの操作は、複数のモードで動作可能なファイル管理プログラムによって主に行われる。このようなモードとしては、セットアップ動作モード、計算機ID動作モード、一時キー導出動作モードがある。セットアップ動作モード時には、ファイル管理プログラムがユーザ制御のデータ処理システムにロードされ、ユーザ制御のデータ処理システム用のオペレーティング・システムに関連付けられる。計算機ID動作モード時には、少なくともユーザ制御のデータ処理システムの属性に基づく数値計算機IDを導出するためにファイル管理プログラムが使用される。一時キー導出

動作モード時には、少なくとも一部が数値計算機IDに基づく一時キーが導出される。また、ファイル管理プログラムにより試用動作モードも可能になり、そのモードでは、一時キーによって定義された期間の間、ソフトウェア・オブジェクトへのアクセスを制限するためにユーザ制御のデータ処理システムでファイル管理プログラムを実行することでそのファイル管理プログラムが使用され、その定義済み期間中は、一時キーを含む少なくとも1つの入力を受取りに対する応答として永続キーを提供するために、ユーザ制御のデータ処理システムで永続キー生成プログラムが使用される。

【0014】ファイル管理プログラムは、データ処理システムのオペレーティング・システム構成要素として提供される。コンピュータがアクセス可能なメモリ媒体には、少なくとも1つの暗号化ファイルと少なくとも1つの非暗号化ファイルとを含む複数のファイルが格納されている。それぞれの暗号化ファイルごとに、事前選択部分がコンピュータ・メモリに記録され、ファイルの暗号解読に使用できる情報を含む暗号解読ブロックが生成され、コンピュータ・メモリの他の場所にすでに記録されている事前選択部分の代わりにその暗号解読ブロックがファイルに組み込まれる。ここでファイル管理プログラムを使用して、アクセス可能なメモリ媒体に格納されている被呼ファイルに関するコンピュータのデータ処理操作呼出しを監視する。ファイル管理プログラムは、その被呼ファイルに関連する暗号解読ブロックを備えているかどうかを判定する。被呼ファイルが関連する暗号解読ブロックを備えているかどうかに応じて、ファイル管理プログラムはその被呼ファイルを特定の方法で処理する。暗号解読ブロックを組み込んだ場合でも暗号化ファイルのサイズは変わらないため、所与のタイプの処理エラーが防止される。試用期間中、暗号化ファイルは暗号化状態に維持されるため、コピーすることができない。潜在的ユーザがソフトウェア製品の購入を決定した場合、暗号解読ブロックの代わりに事前選択部分をファイルに戻すための永続キーが提供される。暗号解読ブロックが除去されると、暗号化ファイルを暗号解読して、購入者による無制限使用を可能にすることができる。オペレーティング・システムによって呼び出されたときにファイル代行受信するために、ならびに、暗号解読ブロックを使用してキー・ファイル用の名前を導出し被呼ファイルを読み取るために、ファイル管理プログラムを使用することが好ましい。それぞれの暗号化ファイルの暗号解読ブロックは、ファイル管理プログラムによって暗号解読され、被呼ファイル用の選択済みセグメントと比較されて、そのキーが特定のファイルを暗号解読できるかどうかを判定するための妥当性検査セグメントを含んでいる。暗号解読された妥当性検査セグメントが既知のクリア・テキスト妥当性検査セグメントと一致すると、ファイルは、今後の処理のためにオペレーティング・システムに渡され

るときに動的に暗号解読される。

【0015】ファイル管理プログラムは、データ処理システムのオペレーティング・システム構成要素として提供される。データ処理システムにとって使用可能でコンピュータがアクセス可能なメモリ媒体には、少なくとも1つの暗号化ファイルと1つの非暗号化ファイルが格納される。この暗号化ファイルには、少なくとも一部が実行可能コードで構成されている非暗号化安全保護スタブが関連付けられている。ここでファイル管理プログラムを使用して、コンピュータがアクセス可能なメモリ媒体に格納されている被呼ファイルに関するデータ処理システム呼出しを監視し、その被呼ファイルが関連の非暗号化安全保護スタブを備えているかどうかを判定し、被呼ファイルが関連の非暗号化安全保護スタブを備えているかどうかに応じて、その被呼ファイルを特定の方法で処理する。より具体的には、被呼ファイルが関連の非暗号化安全保護スタブを備えていないと判定された場合、その被呼ファイルの処理が可能になる。しかし、被呼ファイルが関連の非暗号化安全保護スタブを備えていると判定された場合には、被呼ファイルの処理が可能かどうかの判定を行う前にそのファイルを検査しなければならない。まず、暗号解読操作を実行可能にする情報を得るために、非暗号化安全保護スタブが検査される。次に、暗号解読操作が実行される。最後に、今後の処理のために被呼ファイルの転送が可能になる。被呼ファイルは、処理のためにオペレーティング・システムに渡されるときに動的に暗号解読されること好ましい。また、被呼ファイルの実行前に非暗号化安全保護スタブが被呼ファイルから分離される。ただし、非暗号化安全保護スタブがたまたま被呼ファイルに接続されたままになってしまった場合には、処理操作を停止しなければならない。また、プロセスがロック状態になるのを防止するため、メッセージを通知しなければならない。

【0016】コンピュータがアクセス可能なメモリ媒体は、所定の暗号化エンジンと永続秘密キーとを使用して暗号化されるソフトウェア・オブジェクトを含んでいる。ソースとユーザとの対話を容易にするためのインタフェース・プログラムが提供される。このインタフェース・プログラムは、少なくともユーザ制御のデータ処理システムの所定の属性を使用して計算機IDを生成する計算機IDモジュールを含んでいる。また、このインタフェース・プログラムは、少なくとも一時キーを入力して受け取り、永続秘密キーを出力して生成する永続秘密キー生成プログラムをさらに含んでいる。一時キーをテストしてその妥当性を判定するための妥当性検査モジュールが提供される。ソフトウェア・オブジェクトのソース側は、少なくとも計算機IDを入力として受け取り、一時キーを出力として生成する一時キー生成プログラムを保管している。インタフェース・プログラムはユーザ制御のデータ処理システムにロードされる。ユーザ

制御のデータ処理システムの少なくとも1つの所定の属性を検査し、計算機IDを生成するために、計算機IDモジュールが使用される。この計算機IDは、ソースとユーザとの対話時に不安定な通信チャネルを介してやりとりされる。ソフトウェア・オブジェクトのソース側では、一時キー生成プログラムへの入力として計算機ID（およびその他の情報）を使用して一時キーが生成される。この一時キーは、ソースとユーザとの対話時に、通常、不安定な通信チャネルを介してやりとりされる。次に、妥当性検査モジュールを使用して、一時キーの妥当性を判定する。その後、永続秘密キー生成プログラムを使用して、一時キーを受け取り、ソフトウェア・オブジェクトを暗号解読して一時的にそのオブジェクトへのアクセスを獲得するための永続秘密キーを生成する。一時キーによってソフトウェア・オブジェクトへの一時試行アクセスを可能にする一方で、分散データ処理システム内のある計算機から分散データ処理システム内の別の計算機へ暗号化ソフトウェア・オブジェクト、キー・ファイル、および計算機IDファイルを送送するために携帯用メモリ媒体の使用を可能にするインポート・モジュールとエクスポート・モジュールもユーザに提供される。

【0017】

【実施例】ソフトウェア製品の試用期間での使用を可能にするための本発明の方法および装置は、図1に示すようなスタンドアロン型PCまたは図2に示すような分散データ処理システムで使用できる。いずれの場合にも、1つまたは複数のソフトウェア製品に対する一時試用期間アクセスは、特定のデータ処理システム属性を備えた特定のデータ処理システムにおける試用製品の使い方によって決まる。これは、1つまたは複数のデータ処理システム属性に基づく一時アクセス・キーを使用して試用ソフトウェア製品を暗号化することによって達成される。図3は、以下に詳述する一時アクセス・キーを作成する際に使用可能な複数のシステム構成属性を示したものである。まず、図1のスタンドアロン型データ処理システムの環境と、図2の分散データ処理システムについて詳しく説明し、次に、図3に示す特定のシステム構成属性について説明する。

【0018】ここで添付図面、特に図1に関して説明すると、同図には、本発明によりプログラミング可能なデータ処理システム10の絵画表現が示されている。図示の通り、データ処理システム10は、好ましくはグラフィック・プロセッサと、メモリ装置と、中央処理装置（図示せず）とを含む、プロセス12を含んでいる。このプロセッサ12には、カラー・モニタまたはモノクロ・モニタのいずれかを使用して実現可能な表示装置16が当技術分野で周知の方法で結合されている。また、プロセッサ12にはキーボード14も結合されている。キーボード14は、ケーブルによってプロセッサに結合される標準のコンピュータ・キーボードで構成されるこ

とが好ましい。

【0019】プロセッサ12には、マウス20などの図形ポインティング・デバイスも結合されている。このマウス20は、ケーブルによって当技術分野で周知の方法でプロセッサ12に結合されている。図示の通り、マウス20は、左ボタン24と右ボタン26を含むことができ、そのそれぞれを押す、すなわち「クリック」すると、データ処理システム10にコマンドおよび制御信号を出力することができる。開示されている本発明の実施例ではマウスを使用しているが、当業者は、本発明の方法を実施するためにライト・ペンまたはタッチ画面などの図形ポインティング・デバイスも使用できることに留意されたい。上記の説明を参照する際に、当業者は、IBM製のモデル80PS/2コンピュータなどのいわゆるパーソナル・コンピュータを使用してデータ処理システム10を実現できることに留意されたい。

【0020】本発明はスタンダード型データ処理システムで実施可能であるが、分散データ処理システムでも実施することができる。ただし、その場合は、分散データ処理システム内の特定のデータ処理装置間で携帯メモリ媒体（ディスクまたはテープなど）を介して1つまたは複数の暗号化ファイル、その暗号化キー・ファイル、および関連のファイル管理プログラムを転送するために、本発明のインポート・ルーチンとエクスポート・ルーチンが使用される。本発明のインポート・ルーチンおよびエクスポート・ルーチンについては後で詳述するが、基本的な分散データ処理システムについて説明し、これを理解しておくことが重要である。

【0021】図3は、特定のデータ処理システム（スタンダード型か、分散データ処理システム内のノードか）を明確に識別するのに使用でき、さらに特定の定義済み試用期間の間、暗号化製品へのアクセスを獲得するのに使用できる一時アクセス製品番号を導出または生成する場合に使用する計算機ID値を生成するのに使用できる、複数のデータ処理システム属性を示すブロック図である。データ処理システムは、特定のシステム・バス60アーキテクチャと、特定のメモリ制御装置74と、バス制御装置76と、割込み制御装置78と、キーボード・マウス制御装置80と、DMA制御装置66と、VGAビデオ制御装置82と、並列制御装置84と、直列制御装置86と、ディスク制御装置88と、ディスク制御装置102とを含むことができる。さらに、特定のデータ処理システムを識別するために、複数の空または占有済みスロット106を使用することもできる。それぞれの特定のデータ処理システムは、RAM70、ROM68、またはCMOSRAM72から導出可能な複数の属性を有することができる。計算機ID値を導出するために所定の方法で処理可能な、データ処理システムの1つまたは複数の属性を導出するために、プリンタ96、モニタ94、マウス92、キーボード90、ディス

ケット100、またはディスク・ドライブ104などの端末装置を使用することもできる。この計算機ID値の導出については、後で詳述する。本発明は、ソフトウェア・プログラムのライセンスを（購入することによって）取得する前にそのプログラムを試すための手段をユーザに提供するために、ユーザにソフトウェア・プログラムを配布する効率の良い方法に関するものである。この概念により、ディスクまたはCD-ROMなどのコンピュータがアクセス可能なメモリ媒体に収められた完全なプログラムが潜在的にユーザに配布される。この概念は、ユーザが配布された媒体からプログラムにアクセスできるようにするためのキーを生成することにある。このような環境では、ユーザが各種ソフトウェア製品をブラウズできるようにする複数のインタフェースがファイル管理プログラムによって提供される。このインタフェースにより、配布された媒体に収容されたソフトウェア製品の注文とロック解除が可能になる。ソフトウェア製品のロック解除は、一時アクセス（暗号解説）キーの受取り、妥当性検査、および記録によって達成される。

【0022】ファイル管理プログラムは、ユーザ制御のデータ処理システムに常駐し、ユーザのコンピュータ内でオペレーティング・システムの一部になる。（PC DOS環境における）このような常駐プログラムの一例としては、DOSのファイル入出力操作を代行受償して処理する「終了後常駐」操作のための常駐プログラムTSRが考えられる。ユーザに一時アクセス・キーが提供されると、このファイルが以前は試用動作モードで使用されていたかどうかを確認するため、システム・ファイルが検査される。製品を試用動作モードで使用したことがない場合は、一時キーが保管される。試用動作モード・キーが存在すると、ファイル管理プログラムによって開始された場合のみ、暗号化アプリケーションを実行することができる。この場合、ファイル管理プログラムは、アプリケーションが暗号化され、特定の操作に有効な試用動作モード・キーが存在することを認識する。有効な試用動作モード・キーとは、期限が切れていないキーである。試用動作モードは、タイマまたはカウンタで定義することができる。すなわち、タイマを使用して特定の定義済み期間（たとえば、30日）の砂時計を行うか、あるいはカウンタを使用して、試用動作モード中に許可される定義済み回数分の試用「セッション」の間、減分することができる。キーが有効な場合、ファイル管理プログラムは、TSRと直接やりとりし、特定の暗号化アプリケーションに関して試用動作モードを可能にする。その後、ファイル管理プログラムは暗号化アプリケーションを開始する。ユーザ制御のデータ処理システムのオペレーティング・システムに常駐するコードは、そのオペレーティング・システムに対する制御権を維持する。このコードは、ファイルを暗号解説してメモリにロードできるようにするために試用動作モード・キ

一の使い方を監視するが、暗号化ファイルが暗号解読されて媒体にコピーされるのを防止する。このような操作は、オペレーティング・システムを使用してどのアプリケーションがデータにアクセスしようとしているかを判定し、データへのアクセス許可を持っているアプリケーションだけ、アクセスできるようにすることで行われる。

【0023】図4は、ソフトウェア・オブジェクトを暗号化するためのルーチンを示すブロック図である。ソフトウェア・オブジェクト201を構成する2進キヤクタは、暗号化エンジン205に入力として供給される。暗号化エンジン205では、暗号化キーとして実キー203が使用される。この暗号化エンジン205の出力は暗号化ソフトウェア・オブジェクト207になる。暗号化エンジン205は、公表され既知のDESアルゴリズムなどの従来の暗号化操作である場合もあれば、ソフトウェア・オブジェクト201を乱数化する排他的論理和演算であってもよい。

【0024】図5は、本発明の教示によりソース209（ソフトウェア・ベンダ）とユーザ211（潜在的顧客）との間で行われる情報交換を示す絵画表現である。ソース209とユーザ211との間の矢印は、ベンダ209および211間で行われるオブジェクトまたは情報の交換を意味する。流れ213の交換では、コンピュータがアクセス可能なメモリ媒体がソース209からユーザ211に送られる。この転送は、郵便、宅配便、至急配達によって行われる場合もあれば、書籍や雑誌などの印刷物を介して引き渡される場合もある。あるいは、電子メールまたはその他の伝送技術を使用して、ソース209からユーザ211に電子文書が転送される場合もある。流れ215では、好ましくはユーザ211のデータ処理システムを識別する固有の計算機ID番号を含む、ユーザ固有情報が不安定な通信チャネルを介してユーザ211からソース209に転送される。通常、この情報は電話で交換されるが、電子メールまたはその他の通信技術を使用して渡される場合もある。流れ217では、ソース209がユーザ211に製品キーを提供する。この製品キーを使用すると、所定の定義済み期間の間、メモリ媒体に収容されている製品に一時的にアクセスできるようになる。この期間中は、ユーザ211がそのソフトウェア製品への永続アクセス権を取得するためには、ユーザ211はさらにソース209とやりとりしなければならない。製品キーによって、ユーザ211は特定の定義済み期間の間または特定の定義済み「セッション」数の間、そのソフトウェア製品へのアクセス権を取得することができる。時間の経過とともに、ユーザのクロックまたはカウンタの目盛りが減少する。試用期間が終了すると、それ以上アクセスしようとしても拒否される。この

ため、ユーザ211は、ソース209に連絡するとともに、ユーザ211に送られる、そのソフトウェア製品への無制限アクセスを可能にするために永続的に製品のロックを解除する永続キーを購入するための肯定的ステップを実行しなければならない。

【0025】ソース209とユーザ211との間のやりとりはユーザ・インタフェースによって容易になる。このインタフェースの構築については図6の流れ図に示す。この処理は、ソフトウェア・ブロック219から始まり、ソフトウェア・ブロック221に続く。このブロック221では、ソフトウェア製品の試用期間中の使用の実現を容易にするインタフェースで使用される言語と通貨を決定するための言語および場所の選択がソース209によって行われる。複数のソフトウェア製品をひとまとめにし、コンピュータがアクセス可能な単一のメモリ媒体でユーザ211に配達する場合もある。このため、ソフトウェア・ブロック223により、ソース209は、コンピュータがアクセス可能なメモリ媒体上で試用に供されるプログラムに関する決定を行わなければならない。ソフトウェア・ブロック223により、該当するフィールドが記入される。次に、ソフトウェア・ブロック225により、プログラムが機能的に制限されるか、暗号化される。その後、ソフトウェア・ブロック227により、ディスクまたはCD-ROMなどのコンピュータがアクセス可能なメモリ媒体にコンピュータ・プログラム製品とともにシリアル（ファイル管理プログラムを含む）がロードされる。この処理は、ソフトウェア・ブロック229で終了する。

【0026】図7は、本発明によるベンダと顧客との対話を示す流れ図である。処理の流れは、ソフトウェア・ブロック231から始まり、ステップ233に続く。このステップ233では、試用/購入のための試用期間の間、コンピュータによりアクセス可能なメモリ媒体がユーザに配布される。その後、ステップ235により、コンピュータがアクセス可能なメモリ媒体からユーザ制御のデータ処理システムにファイル管理プログラムがロードされて実行される。このファイル管理プログラムは、ベンダと顧客との間の対話を容易にし、顧客が使用可能なオプションを示す、複数のインタフェース画面を含んでいる。このため、ステップ237により、ファイル管理プログラムが走査検索を可能にし、適切なユーザ・インタフェースを表示する。次に、ステップ239により、通常、電話または電子メールを介して顧客とベンダが対話し、ベンダが顧客に関する情報を収集して、定義済み試用期間の間、コンピュータがアクセス可能なメモリ媒体に収容されている1つまたは複数のソフトウェア製品へのアクセスを可能にする一時キーを配布できるようにする。一般に、この期間中は、内部クロックが、または潜在的購入者が1つまたは複数の特定のソフトウェア製品に対して行うセッションの回数を追跡するカウンタ

によって定義される。ステップ241は、試用期間使用の許可を表している。その後、ソフトウェア・ブロック243により、ファイル管理プログラムは、データ処理システム内のすべての入出力呼出しを監視、監督し、コンピュータがアクセス可能なメモリ媒体に収容されている暗号化ソフトウェア製品の無許可使用を防止する。本発明の好ましい実施例のファイル管理プログラムは、暗号化ファイルへの呼出しを監視し、今後の処理のためにそのファイルが渡される前にアクセスを許可するか、拒否するかを決定する。このため、顧客は、ソフトウェア製品にアクセスして、それを購入するかどうかを決定することができる。その製品の購入を決定した場合は、ステップ245に示すように、顧客はもう一度ベンダと対話しなければならず、ベンダはその顧客に永続キーを引き渡さなければならない。顧客が永続キーを受け取り、購入した1つまたは複数のソフトウェア製品を暗号解読し、そのソフトウェア製品の通常の無制限アクセスが許可されると、処理が終了する。

【0027】図8、図9、図10、および図11は、本発明による試用期間操作を容易にするユーザ・インタフェース画面を示している。図8は、顧客が別のウィンドウから「注文書表示」オプションを選択したときに表示される、注文書ユーザ・インタフェース249を示している。この注文書ユーザ・インタフェース249は、潜在的顧客とベンダとの対話を容易にするためにソフトウェア・ベンダを識別し、電話番号を提供する、タイトル・バー251を含んでいる。試用期間操作中に試すことができる1つまたは複数のソフトウェア製品を識別する注文書フィールド255が設けられている。また、数量サブフィールド259、品目サブフィールド257、説明サブフィールド260、および価格サブフィールド253を含む、複数のサブフィールドも設けられている。削除ボタン261を使用すると、潜在的顧客は注文書フィールドから品目を削除することができる。小計フィールド263は、注文したソフトウェアの価格の小計を示すものである。支払方法アイコン265は、可能な支払形式を識別する。当然のことながら、潜在的ユーザは、電話番号を使ってベンダに直接連絡して、1つまたは複数のソフトウェア製品を購入することができ、あるいは、妥当かどうか判断するためにソフトウェア製品を試す試用期間動作モード用として1つまたは複数のソフトウェア製品を選択することができる。注文書インタフェース249の最下部には、複数の機能アイコン267が設けられている。このようなアイコンとしては、クローズ・アイコン、ファックス・アイコン、メール・アイコン、印刷アイコン、ロック解除アイコン、ヘルプ・アイコンなどがある。ユーザは、従来のポイント・クリック操作で図形ボイディング・デバイスを使用し、これらの操作から1つまたは複数の選択することができる。ファックス・アイコンは、ファックス装置またはファク

ス・ボードを使用してベンダとの対話を容易にするものである。印刷アイコンは、ユーザがソフトウェア・ベンダとの対話を紙に印刷し、保存用コピーを作成できるようにするものである。

【0028】顧客、コンピュータがアクセス可能なメモリ媒体、および顧客が使用するコンピュータ・システムは、媒体ID269、顧客ID273、および計算機ID271によって識別される。媒体IDは、潜在的顧客に発送される前にコンピュータがアクセス可能なメモリ媒体に割り当てられている。このIDは固定されたものであるため、変更できない。顧客ID273は、潜在的顧客とベンダとの対話から導出される。電話での対話中に選択した質問に顧客が回答し、特定の顧客に固有の顧客ID273をベンダが与える方法が好ましい。計算機ID271は、コンピュータがアクセス可能なメモリ媒体に常駐し、潜在的顧客が使用する特定のデータ処理システムに固有のファイル管理プログラムを使用して自動的に導出される。顧客は、通常、電話での対話によりベンダに計算機IDを通知することになるが、ファックスでの対話や郵便での対話も可能である。

【0029】図9は、注文情報ダイアログ・インタフェース275を示す図である。このインタフェースは、潜在的顧客を明確に識別する情報の獲得を容易にするもので、名前フィールド277、住所フィールド279、電話番号フィールド281、ファックス番号フィールド283、支払方法フィールド285、発送方法フィールド287、会員番号フィールド289、有効期限フィールド291、付加価値税IDフィールド293を含んでいる。さらに注文情報ダイアログ・インタフェース275は、潜在的ユーザが上記の各種フィールドから情報を削除したり、インタフェース画面を紙面に印刷できるようにするための印刷ボタン295と取消しボタン297を含んでいる。

【0030】図10および図11は、ロック解除ダイアログ・インタフェース画面301および303を示す図である。ユーザは、図形ボイディング・デバイスを使用して、ロック解除リスト305の構成要素である品目番号フィールド307および説明フィールド309によって識別される1つまたは複数の項目を選択する。このインタフェースはさらに、顧客IDフィールド313と計算機IDフィールド315を含んでいる。電話、ファックス、電子メールまたは郵便による対話でベンダが顧客に顧客IDを与える方法が好ましい。また、ユーザは電話、ファックス、電子メールまたは郵便による対話中に計算機IDフィールド315に計算機IDを入力し、それをベンダに提供することが好ましい。試用期間操作中に要求される製品のIDとともにこの情報が交換されると、キー・フィールド311内に位置する一時アクセス・キーが提供される。このキーは、顧客が識別し選択した製品を一時的にロック解除するためのものである。

ユーザの対話を容易にするため、このインタフェース画面にはクローズ・ボタン319、保管ボタン317、およびヘルプ・ボタン321も設けられている。

【0031】図11は、単一製品ロック解除インタフェース画面303を示す図である。このインタフェース画面は、計算機IDフィールド315、顧客IDフィールド315、およびキー・フィールド311のみを含んでいる。このダイアログは単一製品のみに関するもので、しかも、一時試用期間操作が要求されている製品をユーザが知っているものと想定しているため、ロック解除する製品をこのインタフェースで識別する必要はない。オペレータの対話を容易にするため、このインタフェースには保管ボタン317、取消しボタン319、およびヘルプ・ボタン321も設けられている。

【0032】図12は、試用期間動作モードを開始するために1つまたは複数の暗号化製品をロック解除する際に使用するユーザ・インタフェース画面を示している。図10または図11のいずれかのロック解除ダイアログで「保管」押しボタンを選択すると、図12の開始日ダイアログが表示される。ここでユーザは、日付フィールド310に示されている正しい開始日を確認するよう要求される。ユーザは、「続行」ボタン312、「取消し」ボタン314、または「ヘルプ」ボタン316のいずれかをポイント・クリックすることで、この問合せに回答する。フィールド310に表示される日付は、ユーザ制御のデータ処理システムのシステム・クロックから導出される。この日付を試用期間操作の公式または指定開始日と対応させるために、ユーザがシステム・クロックを変更しなければならない場合もある。

【0033】試用期間操作は2通りの形態が可能である。1つは、ユーザがすべての機能を試せるようにするが、データ・ファイルの印刷や保管などの重要機能は使用不可にするような、機能的に使用不可とする措置が施された製品である。もう1つの試用期間操作は、時間制限を設けて使用可能にした完全機能製品である。この場合はアクセス保護が必要であり、顧客は無料またはわずかな料金で製品のすべての機能を試すことができる。本発明によれば、通常、製品へのアクセスは「期限付き」キーによって制御される。製品を使用するための試用期間は、ベンダが決定した一定期間である。この試用期間はキーが発行されたときから始まる。本発明によれば、試用期間操作中に試用する製品は、顧客シェル内からしか実行できない。暗号解読ドライバは、暗号化製品の明文でのコピーを許可せず、顧客のシェルの外部での実行も許可しない。代替実施例では、顧客がその製品に対して実行する「セッション」ごとに増分または減分されるカウンタによって試用期間が定義される。この場合は、一時キーによる暗号解読が許可されなくなるまでに顧客は定義済み回数だけ製品を使用することができる。

【0034】一時アクセス・キーの制限は、そのキーの

「制御ベクトル」に組み込まれている。通常、制御ベクトルは、そのキーの簡単な説明、計算機ID番号、および試用期間データ（クロック値またはカウンタ値など）を含む定様式テキスト・ストリングを含む。キーを壊さずに制御ベクトルを変更することはできない。保護ソフトウェア製品を実行する場合は、操作試用期間の制限を実施するため、使用データを更新しなければならない。クロックまたはカウンタが不正操作されないように保護するため、その値は、通常は暗号化ファイル内の複数の場所に記録される。本発明の好ましい実施例では、試用期間情報（クロック値またはカウンタ値あるいはその両方）が「キー・ファイル」（後で詳述する）と、計算機IDファイル（これについても後述する）と、システム・ファイルにコピーされる。暗号化プログラムへのアクセスが要求されると、上記の場所がすべて検査され、クロックまたはカウンタあるいはその両方の値が同じであるかどうか判定される。平均的なユーザが3つのファイルすべてを完璧に不正操作できるだけの高度の知識を持っている可能性は低い。好ましい実施例では、クロックとカウンタの組合せを使用して、バックアップの拡大使用と、システム・クロックをリセットするための回復操作を防止している。試用が要求されるたびにPCのクロックをリセットすることは可能であるが、これは、システム上の所与のファイルの日付/時間スタンプを追跡し、ファイルの日付/時間スタンプの中の最新の日付とシステム・クロックとを使用することで検出できる。前述の通り、タイムまたはカウンタあるいはその両方の情報は格納されている3つの場所の1つはシステム・ファイルである。オペレーティング・システムとしてOS/2を使用して操作している場合、時間および使用データは、OS/2内のOS2.INIなどのシステム・データ・ファイルに格納することができる。試用おとび使用データをリセットするには、ユーザはこれらのファイルを連続バックアップし、回復しなければならない。これらのファイルには、ユーザ・システムの動作にとって重要なその他のデータが収容されている。不注意なユーザがこれらのファイルを再フォーマットに回復しようとすると、他のアプリケーションにとって重要なデータを誤って紛失してしまう場合もある。本発明では、上記の保護技法より、不誠実なユーザが許可期間以上に試用期間使用を延長しようとする試みを確実に防止できる。

【0035】大まかに概観すると、本発明では、ベンダがCD-ROMまたは磁気媒体ディスクなどのコンピュータがアクセス可能なメモリ媒体に複数の暗号化ソフトウェア製品をロードする。コンピュータがアクセス可能なメモリ媒体には、ソフトウェア・ベンダソフトウェアの顧客との対話を容易にする複数のユーザ・インタフェース画面を提供する機能など、複数の機能を実行するファイル管理プログラムもロードされる。このコンピュータがアクセス可能なメモリ媒体はユーザ制御のデ

ータ処理システムに装填され、ファイル管理プログラムがロードされて実行される。ファイル管理プログラムは、顧客に関する情報（名前、住所、電話番号、および課金情報）を収集し、試用期間が要求されたソフトウェア製品に関する顧客の選択を受け取るための複数のユーザインタフェース画面を顧客に提供する。ソフトウェア・ベンダと顧客との間では、顧客ID番号、製品ID番号、媒体ID番号、および計算機ID番号などの情報が交換される。ベンダは、独自の内部記録に応じて顧客ID番号を生成する。ソフトウェアの潜在的顧客を識別するために、ソフトウェア・ベンダの担当者は顧客から情報を収集し、その情報を所定の用紙に記入しておくことが好ましい。あるいは、ソフトウェア・ベンダは、記入済みの注文情報ダイアログ・インタフェース画面275

(図9)をファックス、電子メールまたは郵便で受け取ることもできる。配布されたメモリ媒体(CDおよびディスクレットなど)は、少なくとも一部がユーザ制御のデータ処理システムの1つの属性に基づく固有の計算機IDを生成するためのファイル管理プログラムも含んでいる。この計算機IDは、一度限りのセットアップ・プロセス中に作成される8ビットの乱数であることが好ましい。8つのランダム・ビットは、ルーチンの「種」としてシステム時間を使用する基本乱数発生ルーチンから生成されることが好ましい。また、最終結果には検査ビットが付加されていることが好ましい。注文を受け付ける人は電話を介して顧客が読み上げる計算機IDをキー入力しなければならぬので、この検査ビットは注文システムにとって重要である。この検査ビットを使用すると、顧客が番号を反復しなくても、計算機IDを即時確認できる。ユーザ制御のデータ処理システムには、計算機IDのクリア・テキスト(平文テキスト)と計算機IDの暗号化バージョンを収容したマスタ・ファイルが保管されていることが好ましい。

【0036】ソフトウェアの顧客は、ソフトウェア製品の一時試用に関する注文を行う場合、ソフトウェア・ベンダの電話受付に計算機IDを口頭で伝える。それに対して、電話受付は、コンピュータがアクセス可能なメモリ媒体上の暗号化ソフトウェア製品に対する一時アクセス・キーとして機能する製品キーと、顧客ID番号とを顧客に伝える。この製品キーは、計算機IDと、顧客番号と、注文されたプログラム用の実符号化キーと、制御データ・ブロックとの関数であることが好ましい。ソフトウェアの顧客は、製品キーと顧客番号ならびに実符号化キーを作成するための同一制御データ・ブロックを組み合わせることで製品キーを検査することができる。その後、このキーは、比較操作を可能にするために暗号化妥当性検査セグメントの暗号解読に使用される。暗号化妥当性検査セグメントが妥当性検査セグメント用の既知のクリア・テキストと同じであれば、ユーザのファイル管理プログラムは、その製品キーが正しい製品キーであ

り、ソフトウェア製品への一時アクセスに使用できると判断したことになる。このため、比較が一致すれば、そのキーはユーザ制御のデータ処理システムのキー・ファイルに格納される。このキー・ファイルには、製品キーと、顧客キー(顧客番号と内部キー生成キーに基づいて生成される)と、計算機IDを含むクリア・テキスト・ストリングとが収容されていることが好ましい。暗号解読ツールが実符号化キーを導出できるようにするには、この3つの項目がすべてそのまま維持されている必要がある。さらにキー・ファイルがこの特定のユーザ制御のデータ処理システムに結びつけるため、システム・パラメータから導出されたキーを使って同じキー・ファイルが暗号化される。このようなシステム・パラメータは、データ処理システムの構成から導出することができ

【0037】大まかに説明すると、本発明の一時キー(通常は電話により口頭で伝えられる)は、暗号化を使用して実キーと、顧客番号、計算機ID番号、その他の定義済みクリア・テキストとを組み合わせるアルゴリズムによって作成される。したがって、このキーは1台の計算機だけに有効である。つまり、別の人のこのキーを伝えても、その人の計算機上のプログラムはロック解除されないはずである。このため、ソフトウェア・ベンダは、ライセンスによる収入を失うという重大な危険を冒さずに、ディスクレットまたはCD-ROMなどのコンピュータがアクセス可能なメモリ媒体で完全なプログラムを配布して、ソフトウェア・プログラムを販売することができ

【0038】暗号化操作に使用可能なシステムの好ましい固有属性としては、ハード・ディスクの製造番号、ハード・ディスクのサイズとフォーマット、システムの型式番号、ハードウェア・インタフェース・カード、ハードウェアの製造番号、その他の構成パラメータなどがある。この技法の結果、計算機IDファイルは、ユーザ制御のデータ処理システムの同一クローンであるシステム上でしか暗号解読できなくなる。多くのデータ処理システムはそれぞれ構成が異なり、構成を一致させるにはかなり手間がかかるため、同一クローンを入手するのは非常に難しい。この点については、後で詳述する。

【0039】次に図13について説明すると、ファイル管理プログラムは、暗号化ソフトウェア製品とファイル管理プログラムがそこに収容された状態で配布された、コンピュータがアクセス可能なメモリ媒体を受け取る。ファイル管理プログラムは、図13のステップ351に示すように、ユーザ制御のデータ処理システムの構成にアクセスする。ステップ353でデータ処理システムのユーザ固有属性が導出され、計算機ID生成プログラム355への入力として出力される。この計算機ID生成プログラムは、複数の2進文字を入力として受け取って、計算機ID357を表す擬似乱数出力を発生する。乱数発生ルーチン(乱数ジェネレータ)であることが好

ましい。計算機ID生成プログラム355が使用する処理は、複数の2進キャラクタを入力して受け取って、定義済みアルゴリズムにより複数の疑似乱数2進キャラクタを出力として発生する従来の疑似乱数発生ルーチンであればいずれでもよい。

【0040】次に図14に関して説明すると、計算機ID357は、暗号化形式でファイル管理プログラム内にも保管される。計算機ID357は、出力として暗号化計算機ID361を生成するために暗号化エンジン359に人力として供給される。暗号化エンジン359は、DESアルゴリズムなどの規則暗号化ルーチンで構成することができる。暗号化エンジン359には入力としてキー363も供給され、このキー363が従来通り暗号化操作に作用する。キー363はシステム属性セクタ365から導出される。選択候補となるタイプのシステム属性は、ハード・ディスクの製造番号、ハード・ディスクのサイズ、ハード・ディスクのフォーマット、システムの型式番号、ハードウェア・インタフェース・カード、ハードウェアの製造番号、その他の構成パラメータなどを含む、システム属性リスト367を含んでいる。

【0041】本発明では、クリア・テキストの計算機ID357と暗号化計算機ID361がメモリに保管されている。また、本発明では、ファイル管理プログラムが適切なユーザー・インタフェース・画面にクリア・テキストの計算機ID357を通知する。その後、ユーザは、図15のブロック図によりその計算機IDが使用されるソフトウェア・ベンダに計算機IDを連絡する。図示の通り、製品キー暗号化エンジン375はソフトウェア・ベンダの制御下に維持される。この製品キー暗号化エンジン375は、計算機ID357と、顧客番号369（このソフトウェア・ベンダの内部記録機能により顧客に割り当てられているもの）と、実暗号化キー371（顧客の管理下にあるコンピュータがアクセス可能なメモリ媒体上に保管されたソフトウェア製品を暗号化する場合に使用されるもの）と、制御ブロック・テキスト373（定義済みのテキスト部分とすることができる）と、試用期間データ374（試用期間を定義するクロック値またはカウンタ値など）とを入力して受け取る。製品キー暗号化エンジンは、製品キー377を出力として生成する。この製品キー377は、実キー371を暴露するという危険を冒さずに不安定な通信チャネルを介して顧客に伝えることができる。実キー371は暗号化操作によりマスキングされるが、製品キー377を使用できるのは計算機ID357が導出された構成と同一の構成を有するデータ処理システム上に限られるので、暗号化ソフトウェア製品へのアクセスは安全な状態で維持される。

【0042】製品キー377が引き渡されると、ユーザ制御のデータ処理システムに常駐するファイル管理プログラムは、実キー生成プログラム379を使用して、製

品キー377、顧客番号369、制御ブロック・テキスト373、計算機ID357、および試用期間データ374などの複数の入力を受け取る。実キー生成プログラム379は、導出された実キー381を出力として生成する。

【0043】製品キー暗号化エンジン375（図15）と実キー生成構成379（図16）の動作を実行するのに使用する暗号化および暗号解読アルゴリズムについては、1992年10月21日に出版され、"Method and System for Multimedia Access Control Enablement"という名称の関連の米国特許出願第07/964324号に記載されている。

【0044】次に、図17および図18に示すように、ソフトウェア・ベンダによって提供された製品キー377の妥当性および信頼性を判定するため、導出された実キー381がテストされる。図示の通り、導出された実キー381は暗号化エンジン385に一方の入力として供給される。この暗号化エンジン385へのもう一方の入力として、所定の暗号化妥当性検査データ・セグメント383が供給される。暗号化エンジンは、導出されたクリア妥当性検査テキスト387を出力として供給する。その後、図18により、導出されたクリア妥当性検査テキスト387が比較器389で既知のクリア妥当性検査テキスト391と比較される。この比較器389は、導出されたクリア妥当性検査テキスト387と既知のクリア妥当性検査テキスト391との比較をビットごとに行うだけである。導出されたクリア妥当性検査テキスト387が既知のクリア妥当性検査テキスト391と一致すると、ステップ393によりキー・ファイルが作成されるが、導出されたクリア妥当性検査テキスト387が既知のクリア妥当性検査テキスト391と一致しない場合は、ステップ395によりユーザ制御のデータ処理システムに警告が通知される。

【0045】次に図19に移って説明すると、キー・ファイル397は、一時製品キー、顧客キー（顧客番号の暗号化バージョン）、クリア・テキストでの計算機ID番号、および試用期間データ（クロック値またはカウンタ値など）を含むものとして示されている。このキー・ファイルは、暗号化エンジン399に人力として供給される。暗号化エンジン399には、キー401も人力として供給される。キー401は、計算機ID番号を導出する際に使用するシステム属性のような固有のシステム属性403から導出される。暗号化エンジン399は、暗号化キー・ファイル405を出力として提供する。

【0046】図20、図21、図22、図23、および図24は、一時アクセスキーが受け取られ、妥当性が検査され、キー・ファイル397（図19）に記録された後で行われるファイル管理プログラムの操作を示している。

【0047】図20は、暗号化ソフトウェア製品が処理

のためにユーザ制御のデータ処理システムによって呼び出されるときに実行される各種ステップを示すブロック図である。まず、暗号化ファイル405が取り出され、「ヘッダ」部407がユーザ制御のデータ処理システムによって読み取られる。このヘッダは、キー・ファイルの位置を含む複数の構成要素を有する。キー・ファイルの位置は、ステップ409によりキー・ファイルを取り出すために使用される。さらにヘッダは、暗号化妥当性検査テキスト411も含んでいる。この暗号化妥当性検査テキスト411もユーザ制御のデータ処理システムによって読み取られる。前述の通り（および図19に示す通り）、キー・ファイルは製品キー419、顧客キー417、および計算機ID415を含んでいる。図21に示すように、これらは暗号解読エンジン413に入力として与えられる。暗号解読エンジン413は、出力として実キー421を提供する。実キー421を使用して配布されたメモリ媒体上の暗号化ソフトウェア製品を暗号解読する前に、妥当性を判定するためにこの実キーがテストされる。図22は、妥当性検査テストのブロック図である。「ヘッダ」に収容されている暗号化妥当性検査テキスト423は、入力として暗号解読エンジン425に供給される。この暗号解読エンジン425には、実キー421（図21の操作で導出されたもの）も入力として供給される。暗号解読エンジン425は出力としてクリア妥当性検査テキスト427を提供する。図23のブロック図に示すように、クリア妥当性検査テキスト427が入力として比較器429に供給される。この比較器429には、既知のクリア妥当性検査テキスト431も入力として供給される。比較器429は、導出されたクリア妥当性検査テキスト427が既知のクリア妥当性検査テキスト431と一致するかどうかを判定する。テキスト同士が一致すると、ステップ433によりソフトウェア・オブジェクトが暗号解読されるが、妥当性検査テキスト部分同士が一致しない場合は、ステップ435により警告が通知される。図24は、図23のステップ433の暗号解読操作を示すブロック図である。まず、暗号化ソフトウェア・オブジェクト437が入力として暗号解読エンジン439に与えられる。この暗号解読エンジン439には、妥当性検査された実キー441も入力として供給される。暗号解読エンジン439は、出力として暗号解読したソフトウェア・オブジェクト443を供給する。

【0048】暗号化ヘッダは、あるファイルがクリアテキスト・ファイルとともに格納されたときにそのファイルが暗号化されているかどうかの判定に対応するために設けられている。導入時の妥当性検査ステップ（本発明の概念とは一切無関係である）の一部としてファイル・サイズを検査する場合があるので、暗号化ファイルに暗号化ヘッダを設ける際に、ファイル・サイズを変更しないことが重要である。このため、そのファイルのサイズ

を想定以上にする、ソフトウェアの導入時に操作上の困難が発生する場合がある。暗号化製品にアクセスする可能性のある他のソフトウェア・アプリケーションは元のファイル名を使用してそのファイルにアクセスするので、ファイルが暗号化されているという事実を反映するために暗号化ソフトウェア製品に関連するファイル名を変更することができず、そのため、暗号化ヘッダの必要性がさらに増すことになる。したがって、ファイルが暗号化されていることを示すためにファイル名を変更すると、暗号化ソフトウェア製品と他のおそらく関連するソフトウェア製品との有益かつ望ましいやりとりが阻害される恐れがある。たとえば、表計算アプリケーションでは、通常、印刷文書に財務情報を統合できるようにするために関連のワード・プロセッサ・プログラムを表計算の各部を移植することができる。ワード・プロセッサ・プログラム用のハードコード化された元のファイル名を変更すると、これらのソフトウェア製品間の有益なやりとりが阻害される恐れがある。本発明の暗号化ヘッダは、暗号化ファイルとその名前ファイル長で保管し、ソフトウェア製品用のファイル名を未変更の形式で保管することで、上記の問題を解決するものである。

【0049】図25は、暗号化ヘッダ451を備えた暗号化ファイルを示す図である。暗号化ヘッダ451は、固有のID部453、キー・ファイルの名前455、暗号化妥当性検査セグメント457、暗号化タイプ459、サイド・ファイルのオフセット461、暗号化ファイル・データ463などを含む複数のコード・セグメントを含んでいる。当然のことながら、この図の暗号化ファイル・データ463は、ワード・プロセッサ・プログラムまたは表計算などの暗号化ソフトウェア製品を表している。暗号化ヘッダ451は、通常は暗号化ソフトウェア製品の一部を構成するはずの暗号化データの代わりに提供される。また、暗号化ヘッダは、暗号化ソフトウェア製品の最初の部分の位置に代入される。暗号化ファイル・データ463からなる暗号化ソフトウェア製品の前面に暗号化ヘッダ451を配置するためには、暗号化ファイル・データの一部を別の場所にコピーしなければならない。サイド・ファイルへのオフセット461は、移動されたファイル・データが収容されているサイド・ファイル位置を識別するものである。

【0050】図26は、暗号化ファイルのディレクトリとサイド・ファイルとの関係を示す図である。図示の通り、暗号化ファイルのディレクトリ465は、ファイルaaa、ファイルbbb、ファイルccc、ファイルdddからファイルnnnnまでを含んでいる。これらのファイルのそれぞれは、特定の暗号化ソフトウェア製品のディレクトリ名を表している。各暗号化ソフトウェア製品には、ファイルのサイズとファイル名を変更せずに暗号化ヘッダ451を収容するために移動されたファイルの前面部分が入っているサイド・ファイルが関連付けら

れている。ファイルaaaにはサイド・ファイルAAAが関連付けられている。ソフトウェア製品ファイルbbbにはサイド・ファイルBBBが関連付けられている。暗号化ソフトウェア製品cccにはサイド・ファイルCCCが関連付けられている。暗号化ソフトウェア製品dddにはサイド・ファイルDDDが関連付けられている。暗号化ソフトウェア製品nnnにはサイド・ファイルNNNが関連付けられている。図26のディレクトリ名467、469、471、473、475は、サイド・ファイル477、479、481、483、485に関連するものとして示されている。このサイド・ファイルの目的は、ファイル・サイズを変更せずに暗号化ソフトウェア製品のそれぞれに暗号化ヘッダでタグを付けられるようにすることにある。

【0051】暗号化ヘッダ451の暗号化タイプ・セグメント459は、暗号化ソフトウェア製品の暗号化に使用される暗号化のタイプを識別するものである。製品の暗号化にはいくつかある従来の暗号化技法のいずれも使用可能であり、同一メモリ媒体上に収容されている複数の異なるソフトウェア製品を暗号化する場合は異なる暗号化タイプを使用することができる。このため、暗号化タイプ・セグメント459により、暗号化ソフトウェア製品を暗号解読するために適切な暗号化/暗号解読ルーチンが確実に呼び出される。ただし、この場合、一時アクセス・キーが有効で期限切れになっていないことが条件となる。暗号化ヘッダ451のキー・ファイル・セグメントの名前455は、キー・ファイルのアドレス（通常、ディスク・ドライブ位置）を提供する。（図19に関連して）前述の通り、キー・ファイルは、製品キー、顧客キー、およびクリア計算機IDを含んでいる。（図21により）実キーを生成するには、これらの3つの情報がすべて必要になる。暗号化妥当性検査セグメント457は、図23のルーチンを使用して既知のクリア妥当性検査テキストと比較が可能な導出済みクリア妥当性検査テキストを生成するための図22に示すルーチンで使用される暗号化妥当性検査テキストを含んでいる。導出されたクリア妥当性検査テキストが既知のクリア妥当性検査テキストと完全に一致する場合のみ、導出された妥当性検査された実キーを使用して図24により暗号化ソフトウェア製品を暗号解読することにより、処理を続行することができる。しかし、図24の暗号解読操作を実行する前に、暗号化ヘッダ451の代わりに対応するサイド・ファイルの内容を暗号化ソフトウェア製品に戻しておかなければならない。これにより、暗号解読操作の前に暗号化ソフトウェア製品が完全なものになる。

【0052】ユーザ制御のデータ処理システムのオペレーティング・システムによる処理のためにファイルが呼び出されるたびに、そのオペレーティング・システムに常駐するファイル管理プログラムが入出力要求を代行受信（intercept）し、ファイルの前面部分を検査して、

固有のID453のような暗号解読ブロックIDが特定の既知の場所に存在するかどうかを判定する。パフォーマンスを最善にするため、図25に示すように、通常、この場所はファイルの先頭になる。ファイルが暗号解読ブロックを備えているファイル管理プログラクが判定すると、TSR（終了後常駐もしくは常駐型プログラム）がそのブロックをメモリに読み込む。その後、キー・ファイルが入っているドライブおよびディレクトリを指定する環境変数をコピーし、暗号化ブロックからのキー・ファイル名を連結することで完全修飾キー・ファイル名を作成するために、その暗号解読ブロックが解析される。次に、TSRはキー・ファイルのオープンを試みる。キー・ファイルが存在しない場合は、TSRは、暗号化ファイルのオープンを試みているアプリケーションに「アクセス拒否」応答を返す。キー・ファイルが存在すると判定された場合は、TSRはキー・ファイルをオープンし、各種のキー（製品キー、顧客キー、および計算機ID）を読み込んで、実キーを生成する。この実キーは、暗号解読ブロック妥当性検査データを暗号解読するために使用されている。前述の通り、比較操作によって、この暗号解読操作が正常に行われたかどうかが判定される。比較が失敗に終わった場合、キー・ファイルは「無効」と判定され、暗号化ソフトウェア製品のオープンを試みているアプリケーションに対してTSRが「アクセス拒否メッセージ」を返す。しかし、比較が正常に行われた場合は、ファイル管理プログラムは、暗号化ヘッダで検出された暗号化タイプに応じてファイルの暗号解読の準備を行う。その後、ファイルがオープンされたことを示すために、TSRは有効なファイル・ハンドルを呼び出し側アプリケーションに返す。アプリケーションが暗号化ファイルからデータを読み取る場合、TSRは、アプリケーションに戻す前にこのデータを読み取って暗号解読する。要求されたデータがサイド・ファイル内に格納されている移動済みデータの一部分である場合は、データが別のファイルからのものであることを呼び出し側アプリケーションに知らせずに、TSRがサイド・ファイルを読み取って、適切な暗号解読済みブロックを呼び出し側アプリケーションに返す。

【0053】図25および図26では暗号化ヘッダの大きな概念を示したが、図27、図28、および図29では暗号化ファイルの作成に関するより詳細な態様を示す。図28および図29は、2種類のデータ・ファイルを示している。図28は非実行データ・ファイルを示しているのに対し、図29は実行データ・ファイルを示している。また、図27は、シグナチャ・セグメント501、ヘッダLEN503、サイド・ファイル・インデックス505、サイド・ファイルLEN507、暗号解読タイプID509、検証データ511、およびキー・ファイル名518を含むヘッダ499を示している。図28に示すように、ソフトウェア製品はクリア・ファイル5

21として始まり、特定の暗号化ルーチンにより暗号化ファイル523に暗号化される。クリア・ファイル521を暗号化ファイル523に変更する場合に使用される暗号化のタイプは、ヘッダ499の暗号化タイプ・セグメント509によって識別される。次に、暗号化ファイル523の前面部分が、ヘッダ499のサイド・ファイル・インデックス505とサイド・ファイルLEN507によって識別されるサイド・ファイル527にコピーされる。さらに、サイド・ファイル527には、検証データのクリア・テキストのコピーも含まれる。その後、修正済み暗号化ファイル525を形成するためにヘッダ499が暗号化ファイル523の前面部分にコピーされる。図29に示すように、実行ファイルについても同様の処理が行われる。暗号化ファイル533を形成するために、ソフトウェア製品のクリア・テキスト・コピー（クリア・ファイル531として表されているもの）が従来のルーチンにより暗号化される。暗号化ファイル533のデータの重なり（オーバーレイ）が防止されるように、暗号化ファイル533の前面部分がサイド・ファイル539にコピーされる。しかも、サイド・ファイル539は、検証データのクリア・テキストのコピーを含む。その後、暗号化ファイル533の最初の部分（前面部分）に実行可能スタブ537とヘッダ599をオーバーレイすることで、暗号化ファイル533が修正される。

【0054】ここで図29の実行可能スタブ537の目的について説明する。パーソナル・コンピュータ用のDOSオペレーティング・システムは、暗号化アプリケーションの実行を試みる。その結果、システムが「ハング」したり、好ましくないアクションを起こす場合がある。図29の実行ファイルの実行可能スタブ537は、暗号化されたアプリケーションの実行をユーザが試みないようにするために使用される。つまり、ユーザが暗号化ファイルを実行しようとする、システムをハングさせたり、ドライブをフォーマットしたりする危険性がかなり大きいと思われる。導入済みTSRを使用せずにアプリケーションを実行したり、TSRが「監視」していないドライブからアプリケーションを実行した場合に必ず実行可能スタブが実行されるように、このスタブは暗号化ソフトウェア製品の前面部分に接続されている。このスタブによって、アプリケーションを実行できない理由を説明するメッセージがユーザに通知される。この実行可能スタブを使用すると、メッセージの提供以外に、次のような高度なアクションを実行することができる。

(1) TSRの機能性を復元し、もう一度アプリケーションを開始する前に動的暗号化を導入することができる。

(2) 一時アクセス・キーをオンにして、もう一度アプリケーションを開始することができる。

(3) TSRとやりとりして、アプリケーションの実行元であるドライブを調べるよう通知することができる。

【0055】実行可能スタブは、暗号化プログラムに次のように保管またはコピーされる。

(1) アプリケーションを暗号化する。

(2) このプログラム用に暗号解読ブロックを作成する。

(3) 暗号解読ブロックの前面部分に事前作成実行可能スタブが接続される。

(4) 結合した暗号解読ヘッダと実行可能スタブの長さを求める。

(5) 実行可能ファイルの前面にあつてこの長さに匹敵するバイト数がメモリ、好ましくは定義済みのサイド・ファイル位置に読み込まれる。

(6) 暗号化ヘッダと実行可能スタブが実行可能コードの先行バイトの上に書き込まれる。

【0056】TSRは、実行可能スタブの「既知のサイズ」を超えて暗号解読ブロック部分を探索することで、実行可能スタブが暗号化されているかどうかを判定できる。TSRは、実行可能スタブを暗号解読するときに、サイド・ファイルにアクセスし、スタブとヘッダ・ブロックによって移動されたバイトを読み込む。

【0057】図30および図31は、試用期間中の操作を示す流れ図であり、この操作はソフトウェア・ブロック601から始まる。ソフトウェア・ブロック603により、ユーザ制御のデータ処理システムのオペレーティング・システム内に位置するファイル管理プログラムがメモリ媒体への入出力呼出しを連続監視する。その後、ソフトウェア・ブロック605により、各入出力呼出しごとに被呼ファイルがファイル管理プログラムにより代行受信され、ソフトウェア・ブロック607により、アクセスを許可すべきかどうかをファイル管理プログラムが判定できるようになるまで、オペレーティング・システムから被呼ファイルへのアクセスが拒否される。被呼ファイルのうち、暗号解読ブロックが位置するはずの部分が読み取られる。その後、ソフトウェア・ブロック609により、被呼ファイルのこの部分が読み出され、ソフトウェア・ブロック611により、キー・ファイル・アドレスが導出される。導出されたアドレスは、ソフトウェア・ブロック613によりキー・ファイルを取り出す際に使用される。判定ブロック615の結果、キー・ファイルを読み止められない場合は、ソフトウェア・ブロック617で処理が終了する。しかし、判定ブロック615により、キー・ファイルを読み止めることができると判定された場合は、ソフトウェア・ブロック619によりキーが導出される。その後、ソフトウェア・ブロック621により、導出されたキーを使用して、暗号化ヘッダ内に位置する妥当性検査セグメントが暗号解読される。判定ブロック623では、暗号解読妥当性検査セグメントが暗号解読妥当性検査セグメント用のクリア・テキストと比較される。暗号解読されたセグメントが既知のクリア・テキスト・セグメントと一致しない場合

は、処理はソフトウェア・ブロック625に続き、終了する。しかし、判定ブロック623で、暗号解読された妥当性検査セグメントが既知のクリア・テキスト妥当性検査セグメントと一致すると判定されると、処理はソフトウェア・ブロック627に続き、そこで被呼ファイルへのアクセスが許可される。次に、ソフトウェア・ブロック629により、暗号解読ヘンダから暗号解読タイプが読み取られ、ソフトウェア・ブロック633によりユーザ制御のデータ処理システムのオペレーティング・システムによる処理のために渡したときに、被呼ファイルがソフトウェア・ブロック631により動的に暗号解読される。処理はソフトウェア・ブロック635で終了する。

【0058】暗号化ファイルの無許可実行を試みると、実行可能スタブは少なくとも一時的にアクセスを拒否し、システムにメッセージを通知するが、前に挙列したいくつかの高度な方法で問題を処理することができる。

【0059】本発明の好ましい実施例によれば、見込みのある購入者は、試用期間中または試用期間終了時に、コンピュータがアクセス可能なメモリ媒体上の1つまたは複数のソフトウェア製品のコピーの購入準備のためにベンダに連絡する可能性がある。潜在的ユーザに製品を発送するためにCD-ROMまたはフロッピー・ディスクが使用されていることが好ましい。また、コンピュータがアクセス可能なメモリ媒体は、試用期間中に提供される各製品について暗号化したコピーを2つ含むことが好ましい。一方の暗号化コピーは、ファイル管理プログラムと、ベンダから購入者に通知される一時キーとを使用して暗号解読することができる一次的なものである。もう一方の暗号化コピーは、試用期間動作モードでの使用を目的として提供されるのではなく、ソフトウェア製品の購入後に暗号解読と使用が可能になる永続コピーとして提供されるものである。大まかに概説すると、ユーザは、試用期間動作モード用にソフトウェア製品を選択し、(ファイル管理プログラムにより)定義済み試用期間中の製品へのユーザ・アクセスを可能にする一時アクセス・キーをベンダから取得する。試用期間終了前または終了後にユーザは、ファックス、電子メール、または電話によってベンダに連絡することで、ソフトウェア製品の永続コピーをベンダから購入することができる。支払を受け取ると、ベンダは、ソフトウェア製品のうち1つの暗号化コピーを暗号解読するのに使用する永続アクセス・キーをユーザに通知する。この暗号化製品は、DESアルゴリズムなどの従来の暗号化ルーチンを使用して暗号化することができる。永続キーにより、ソフトウェア製品を暗号解読して無制限に使用することができる。1回のランゼーションで1つの製品の複数のコピーを購入する場合があるため、本発明は、可動アクセス・キーを提供するための技法を備えている。この可動アクセス・キーについては、図32～図37に関連して後

述する。本発明の好ましい実施例で使用するソフトウェア製品の上述の第2のコピーを暗号化し暗号解読するための暗号化アルゴリズムは、試用期間動作モードで使用するものと同様である。

【0060】本発明は、試用期間終了後に永続アクセス・キーの配布に対応するためのエクスポート(送信)/インポート(受信)機能を含んでいる。通常、オフィスの管理者またはデータ処理システムの管理者は、試用期間終了後に暗号化製品の指定数の複数の「コピー」を購入する。その後、組織内の所与の個人に対し、暗号化製品への無制限かつ永続的なアクセスを可能にする永続キーが発行される。分散データ処理ネットワーク内に計算装置が接続されていないオフィスや作業環境では、オフィスの管理者またはデータ処理システムの管理者から、組織内で暗号化ソフトウェア製品のコピーの受取りが予定されている指定の個人に対し、永続アクセス・キーを通知しなければならない。永続キーは製品への永続的アクセスに対応するものである。特定の暗号化製品のコピーを組織内のすべての従業員に発行できるわけではないので、ベンダとしては、売買契約またはライセンス契約を超えるような配布を最小限に抑えるか防止するような配布方法を希望するはずである。製品は暗号化されているため、暗号化した形式であれば自由に配布することができる。本発明で保護の対象となるのは、製品への無制限アクセスを可能にする各種キーである。電子メールや印刷物のやりとりでキーが配布されるのを防止するため、本発明は、ソース・コンピュータに常駐するエクスポート・プログラムと、ターゲット・コンピュータに常駐するインポート・プログラムとを含み、これらのプログラムにより、フロッピー・ディスクなどの取外し可能メモリ媒体を介して行われるアクセス・キーの配布に対応している。このため、アクセス・キーが不注意や事故によって配布または開示されることはなくなる。この目標を達成するための主な実施例は2通りある。

【0061】第一の実施例では、ソース・コンピュータに保管されている1つまたは複数の暗号化ファイルがまず暗号解読され、次に暗号化アルゴリズムと移送可能メモリ媒体に固有の暗号化キー(ディスクの製造番号など)を使用して、そのファイルが暗号化される。キー・ファイルはディスクによってターゲット・コンピュータに物理的に運搬することができ、そのターゲット・コンピュータでは転送可能メモリ媒体との対話によりターゲット・コンピュータが導出したキーを使用してキー・ファイルの暗号解読が行われる。その後直ちに、ターゲット・コンピュータの固有のシステム属性から導出されたキーで鍵がかけられた暗号化操作を使用して、キー・ファイル(複数可)の暗号化が行われる。

【0062】第二の実施例では、ターゲット・コンピュータに明確に関連付けられ、ターゲット・コンピュータの1つまたは複数の固有のシステム属性から導出可能な

転送キーをターゲット・コンピュータのインポート・ファイルから獲得するために、転送可能メモリ媒体がターゲット・コンピュータに装填される。その後、メモリ媒体はソース・コンピュータに転送され、そこで1つまたは複数のキー・ファイルが暗号解読され、さらに転送キーを使用して暗号化される。次に、メモリ媒体はターゲット・コンピュータに運搬され、そこで転送キーが生成され、1つまたは複数のキー・ファイルを暗号解読するための暗号解読操作で転送キーが使用される。ターゲット・コンピュータに明確に関連付けられ、1つまたは複数の固有のコンピュータ構成属性から導出可能なキーで鍵がかけられた暗号化操作を使用して、直ちにキー・ファイルの暗号化が行われることが好ましい。第一の実施例については、図32、図33、図34、および図35に関連して説明する。また、第二の実施例については、図36および図37に関連して説明する。

【0063】図32および図33は、別のシステムへのインポートが可能になっているアクセス・キーの固有のディスク・イメージを生成する「エクスポート」機構を使用して、許可ユーザが永続キーを別のデータ処理システムへ移動できるようにするためのエクスポート操作とインポート操作をブロック図形式で示したものである。本発明によれば、ソフトウェア・ベンダから顧客に電話で引き渡されるアクセス・キーの長さは40バイト未満である。生成されたキー・ファイルの長さは2000バイトを上回る。キー・ファイルと計算機IDファイルはディスクにコピーするためのエクスポート機構が設けられている。誰でも使用可能な公共フォーラムにコピーされるのを禁止するために、両方のファイルは、修正済みのディスク製造番号で暗号化される。別のシステムに設けられているインポート機構は、これらのファイルを暗号解読し、ディスクから得た製品キーと計算機IDをインポート・システム・マスタ・ファイルのインポート製品キーおよび計算機IDのリストに追加し、そのキー・ファイルをインポート・システム・ハード・ディスクにコピーする。前に開示したとおり、このキー・ファイルがインポート・システム上で暗号化される。

【0064】図32は、本発明の好ましい実施例によるエクスポート操作を示すブロック図である。図示の通り、ソース・コンピュータ651は、キー・ファイル653と計算機IDファイル655を含む。キー・ファイル653は、製品キーと、顧客キーと、ソース・コンピュータ651用の計算機IDのクリア・テキストと、試用期間データ（試用期間を定義するクロックまたはカウンタあるいはその両方など）と、特定の保護ソフトウェア製品について許可されたエクスポート操作の最大数を定義し、実施されたエクスポート操作の総数を追跡するという二重機能を実行するエクスポート・カウンタを含む。計算機IDファイルは、計算機ID番号と試用

期間データ（試用期間を定義するクロックまたはカウンタあるいはその両方など）を含む。キー・ファイル653と計算機IDファイル655はどちらも従来の暗号化操作（DESアルゴリズムなど）によって暗号化されるが、この操作はソース・コンピュータ651の固有のシステム属性から導出されるキーで鍵がかけられている。エクスポート操作の開始時に、キー・ファイル653と計算機IDファイル655が暗号解読される。キー・ファイル653は、キー659で鍵がかけられた暗号解読操作657に入力として供給される。同様に、計算機IDファイル655は、キー661で鍵がかけられた暗号解読操作663に入力として供給される。暗号解読操作657および663は、キー・ファイル653と計算機IDファイル655のクリア・テキスト・バージョンを生成する。クリア・テキストが得られると、キー・ファイル653内に収容されているエクスポート・カウンタがブロック661により修正される。たとえば、この操作が、許される10回の操作のうちの7回目のエクスポート操作であれば、カウンタは「7:10」と表示するはずである。キー・ファイル653のクリア・テキスト・バージョンは暗号化操作669に入力として供給される。この暗号化操作669は、従来のいずれかの暗号化操作（DESアルゴリズムなど）でもよく、修飾子667による修正の対象となったソース・コンピュータ651に結合されたメモリ媒体に固有のメモリ媒体属性665で鍵がかけられる。たとえば、メモリ媒体677に固有の「メモリ媒体属性」として固有のディスク製造番号を供給することができる。わずかに変更して暗号化操作669に入力として供給するために、ディスク製造番号は修飾子667により修正される。計算機IDファイル655のクリア・テキストについても同じ操作が行われる。すなわち、固有のメモリ媒体属性677が修飾子673によって修正され、暗号化操作675のキーとして使用される。この暗号化操作は、DES操作などの従来の暗号化操作で構成することができる。最後に、暗号化操作669および675の出力がコピー操作679および681に入力として供給され、暗号化キー・ファイル653と計算機IDファイル655がメモリ媒体677にコピーされる。

【0065】図33は、インポート操作を示すブロック図である。メモリ媒体677（図32）はソース・コンピュータ651（図32）から物理的に取り外され、コンピュータ707（図33）に物理的に運搬される。あるいは、分散データ処理システムではこの転送は、メモリ媒体677の物理的な取外しを伴わずに行われる場合もある。ここで図33に関して説明すると、どの特定のターゲット・コンピュータがキー・ファイルと計算機IDファイルを受け取ったかを記録するために、ブロック683により、ターゲット・コンピュータの計算機IDがメモリ媒体677にコピーされる。次に、ブロック6

85および693により、暗号化キー・ファイル653と計算機IDファイル655がメモリ媒体からターゲット・コンピュータ707にコピーされる。暗号化キー・ファイル653は、キー687で鍵がかけられた暗号解読操作689が入力として供給される。暗号解読操作689は、ブロック669の暗号化操作を取り消すもので、キー・ファイル653のクリア・テキスト・バージョンを出力として提供する。同様に、計算機IDファイル655は、キー695で鍵がかけられた暗号解読操作697が入力として供給される。暗号解読操作697は、暗号化操作675の暗号化を取り消すもので、計算機IDファイル655のクリア・テキストを出力として提供する。ブロック691により、ソース・コンピュータ651の計算機IDが取り出され、キー・ファイル653のクリア・テキストとしてメモリ内に記録される。次に、キー・ファイル653のクリア・テキストが暗号化操作699に入力として供給される。暗号化操作699は、DES操作などの従来の暗号化操作であり、ターゲット・コンピュータ707用の計算機IDまたは修正済み計算機IDなどのターゲット・コンピュータ固有の属性で鍵がかけられている。計算機IDファイル655のクリア・テキストは、暗号化操作703に入力として供給される。この暗号化操作703は、DES暗号化操作などの従来の暗号化操作であり、ターゲット・コンピュータ707の計算機IDまたは修正済み計算機IDなどの固有のターゲット・コンピュータ属性705で鍵がかけられている。暗号化操作699の出力は、製品キー（ソース・コンピュータ651のキー・ファイル653の一時製品キーと同じ）、顧客番号（ソース・コンピュータ651のキー・ファイル653の顧客番号と同じ）、クリア計算機ID（ターゲット・コンピュータ707用の計算機IDであって、ソース・コンピュータ651の計算機IDではない）、試用期間データ（ソース・コンピュータ651のキー・ファイル653の試用期間データと同じ）、およびソース・コンピュータ651の計算機IDのIDを含む暗号化キー・ファイル709を生成する。暗号化操作703の出力は計算機IDファイル711を定義するもので、このファイルは、ターゲット・コンピュータ707の計算機ID（ソース・コンピュータ651の計算機IDではない）と試用期間データ（ソース・コンピュータ651の計算機IDファイル655の試用期間データと同じ）とを含む。

【0066】図34および図35は、図32および図33に示したインポート操作とエクスポート操作の代替図で、本発明の重要な特徴の一部を強調するものである。図示の通り、ソース・コンピュータ801は、ソース・コンピュータ801に固有のシステム属性キーで暗号化された計算機IDファイル803を含む。この計算機IDファイルは、計算機IDファイル番号ならびに各保護ソフトウェア製品ごとに許されるエクスポートの回数を

示すカウントと、使用されたエクスポートの総数を示すカウントとを含む。たとえば、最初のエクスポート操作で“1:10”というカウントが伝達された場合、許可された10回のエクスポート操作のうちの1回が行われたことを意味する。次のエクスポート操作では、カウンタは“2:10”に増加し、許可された10回のエクスポート操作のうち2回が行われたことを意味する。特定のエクスポート操作の受取り側であることを示すために、エクスポート操作の結果を受け取る各ターゲット・コンピュータには、この特定のカウンタ値でタグが付けられる。たとえば、1つのソース・コンピュータ・システムが“1:10”というカウンタ値を有する場合、このシステムが許可された10回のエクスポート操作のうちの最初のエクスポート操作の受取り側であることを意味する。さらに別のターゲット・コンピュータが“7:10”というカウンタ値を有する場合は、この特定のターゲット・コンピュータが許可された10回のエクスポート操作のうちの7回目のエクスポート操作を受け取ったことを意味する。このようにして、ターゲット・コンピュータは使用したエクスポート操作の総数のカウンタを保管するのに対し、それぞれのソース・コンピュータは、許可された複数のエクスポート操作のうちの特定の操作による計算機IDファイルとキー・ファイルの受取り側を識別するための異なるカウンタ値を有する。

【0067】ソース・コンピュータ801では、ソース・コンピュータ801に固有のシステム属性をキーとして使用する暗号化アルゴリズムによって計算機IDファイル803とキー・ファイル805が暗号化されるが、計算機IDファイル803とキー・ファイル805がエクスポート・キー・ディスクセット807などのメモリ媒体に転送されると、ディスクセットの製造番号などの固有のディスクセット属性を暗号化キーとして使用する従来の暗号化操作で計算機IDファイル809とキー・ファイル811が暗号化されることに留意されたい。これにより、計算機IDファイル809またはキー・ファイル811あるいはその両方の内容が別のディスクセットまたは他のメモリ媒体にコピーされ、ソフトウェア製品の無許可アクセスを獲得するのに利用される可能性が最小限に抑えられる。その理由は、計算機IDファイル809とキー・ファイル811の内容を効果的にターゲット・コンピュータに転送するために、ターゲット・コンピュータはエクスポート・キー・ディスクセット807から固有のディスクセット属性を読み取って使用できなければならないためである。計算機IDファイル809とキー・ファイル811がコピーされているディスクセットでこれらのファイルがターゲット・コンピュータに提供された場合のみ、効果的な転送を行うことができる。暗号解読操作を正常に実施するにはターゲット・コンピュータはエクスポート・キー・ディスクセット807の固有の属性（ディスクセット製造番号など）を必要とするため、潜在

的ターゲット・コンピュータに対してエクスポート・キー・ディスクセット807以外のディスクセットで計算機IDファイル809とキー・ファイル811を提供すると、無意味な情報が転送されてしまう。

【0068】図35に示すように、エクスポート・キー・ディスクセット807はターゲット・コンピュータ813に提供される。当然のことながら、計算機IDファイル809とキー・ファイル811は暗号化形式になっている。エクスポート・キー・ディスクセット807からターゲット・コンピュータ813に転送する場合、計算機IDファイル809の内容は、ターゲット・コンピュータ813の計算機IDと、使用したインポート操作のカウントで更新される。ターゲット・コンピュータ813への転送を実施する場合、ターゲット・コンピュータ813用の計算機IDなどの複数の項目と、顧客情報、ならびにソース・コンピュータ801の計算機ID番号のリストを含む計算機IDファイル815が作成される。計算機IDファイル815とキー・ファイル817はどちらも、ターゲット・コンピュータ813の固有の属性をキーとして使用する従来の暗号化操作を使用して暗号化される。これにより、計算機IDファイル815およびキー・ファイル817が特定のターゲット・コンピュータ813に結びつけられる。

【0069】エクスポート/インポート・カウントを使用して、許可されたエクスポート/インポート操作の総数と使用したエクスポート/インポート操作の総数を追跡することで、本発明は、試用期間中にソフトウェア製品の配布を追跡するのに使用可能な監査証跡 (audit trail) を作成する。各ソース・コンピュータは、実行されたエクスポート操作の総数の記録を保有する。また、各ソース・コンピュータは、どの特定のエクスポート/インポート操作が1つまたは複数の保護ソフトウェア製品をターゲット・コンピュータに転送するのに使用されたかについての記録も保有する。この転送を実施するのに使用するメモリ媒体 (1枚のディスクセットまたは1群のディスクセットなど) は、すべてのエクスポート/インポート操作に使用されたソース・コンピュータとターゲット・コンピュータの両方の計算機ID番号の永続的記録を保有する。

【0070】エクスポート操作とインポート操作を実施するための手順により、保護ソフトウェア製品が不必要な危険に曝されることがなくなる。計算機IDファイルとキー・ファイルがソース・コンピュータからターゲット・コンピュータに渡されると、エクスポート・ディスクセットをコピーしたり、不当にキーを配布するための手段としてその内容を掲示板に掲載する行為を防止または禁止するエクスポート・ディスクセットの固有の属性によって、これらのファイルが暗号化される。インポート操作時は、ソース・コンピュータの安全保護と一致するようにソフトウェア製品が維持されることを保証するた

め、計算機IDファイルとキー・ファイルがターゲット・コンピュータに固有のシステム属性で暗号化される。ただし、ソフトウェア製品そのものはターゲット・コンピュータに固有の属性で暗号化される。その結果、キーの不当コピーや掲載が防止される。

【0071】エクスポート/インポート機能の第二の実施例は、図36および図37にブロック図形式で示す。大まかに概説すると、まず、メモリ媒体1677を使用してターゲット・コンピュータ1707とやりとりし、ターゲット・コンピュータ1707に固有で、好ましくはターゲット・コンピュータ1707の1つまたは複数の固有のシステム属性から導出される転送キーをターゲット・コンピュータ1707から獲得する。この転送キーは、ターゲット・コンピュータ1707用の計算機IDの修正版でもよい。次に、メモリ媒体1677を使用してエクスポート動作モードでソース・コンピュータ1651とやりとりする。そのモードではキー・ファイル1653と計算機IDファイル1655がまず暗号解読され、その後、転送キーを使用して暗号化される。

【0072】図36は、本発明の好ましい実施例によるエクスポート操作を示すブロック図である。図示の通り、ソース・コンピュータ1651は、キー・ファイル1653と計算機IDファイル1655とを含む。キー・ファイル1653は、製品キーと、顧客キーと、ソース・コンピュータ1651用の計算機IDのクリア・テキストと、試用期間データ (試用期間を定義するクロックまたはカウンタあるいはその両方など) と、特定の保護ソフトウェア製品について許可されたエクスポート操作の最大数を定義し、実施されたエクスポート操作の総数を追跡するという二重機能を実行するエクスポート・カウントを含む。計算機IDファイルは、計算機ID番号と試用期間データ (試用期間を定義するクロックまたはカウンタあるいはその両方など) とを含む。キー・ファイル1653と計算機IDファイル1655はどちらも従来の暗号化操作 (DESアルゴリズムなど) によって暗号化されるが、この操作はソース・コンピュータ1651の固有のシステム属性から導出されるキー鍵がかけられている。エクスポート操作の開始時に、キー・ファイル1653と計算機IDファイル1655が暗号解読される。キー・ファイル1653は、キー1659で鍵がかけられた暗号解読操作1657に入力して供給される。同様に、計算機IDファイル1655は、キー1661で鍵がかけられた暗号解読操作1663に入力して供給される。暗号解読操作1657および1663は、キー・ファイル1653と計算機IDファイル1655のクリア・テキスト・バージョンを生成する。クリア・テキストが得られると、キー・ファイル1653内に収容されているエクスポート・カウントがブロック1661により修正される。たとえば、この操作が、許される10回の操作のうちの7回目のエクスポート

ト操作であれば、カウンタは”7:10”と表示するはずである。キー・ファイル1653のクリア・テキスト・バージョンは暗号化操作1669に力入として供給される。この暗号化操作1669は、従来のいずれの暗号化操作(DESアルゴリズムなど)でもよく、前に得られた転送キー1665で鍵がかけられる。計算機1Dファイル1655のクリア・テキストについても同じ操作が行われる。すなわち、転送キー1671が暗号化操作1675のキーとして使用される。この暗号化操作は、DES操作などの従来の暗号化操作で構成することができる。最後に、暗号化操作1669および1675の出力がコピー操作1679および1681に力入として供給され、暗号化キー・ファイル1653と計算機1Dファイル1655がメモリ媒体1677にコピーされる。

【0073】図37は、インポート操作を示すブロック図である。メモリ媒体1677(図36)はソース・コンピュータ1651(図36)から物理的に取り外され、コンピュータ1707(図37)に物理的に運搬される。あるいは、分散データ処理システムではこの転送は、メモリ媒体1677の物理的な取外しを伴わずに行われる場合もある。ここで図37に関して説明すると、どの特定のターゲット・コンピュータがキー・ファイルと計算機1Dファイルを受け取ったかを記録するために、ブロック1683により、ターゲット・コンピュータの計算機1Dがメモリ媒体1677にコピーされる。次に、ブロック1685および1693により、暗号化キー・ファイル1653と計算機1Dファイル1655がメモリ媒体からターゲット・コンピュータ1707にコピーされる。暗号化キー・ファイル1653は、キー1687で鍵がかけられた暗号解読操作1689に力入として供給される。暗号解読操作1689は、ブロック1669の暗号化操作を取り消すもので、キー・ファイル1653のクリア・テキスト・バージョンを出力として提供する。同様に、計算機1Dファイル1655は、キー1695で鍵がかけられた暗号解読操作1697に力入として供給される。暗号解読操作1697は、暗号化操作1675の暗号化操作を取り消すもので、計算機1Dファイル1655のクリア・テキストを出力として提供する。ブロック1691により、ソース・コンピュータ1651の計算機1Dが取り出され、キー・ファイル1653のクリア・テキストとしてメモリ内に記録される。次に、キー・ファイル1653のクリア・テキストが暗号化操作1699に力入として供給される。暗号化操作1699は、DES操作などの従来の暗号化操作であり、ターゲット・コンピュータ1707用の計算機1Dまたは修正済み計算機1Dなどのターゲット・コンピュータ固有の属性で鍵がかけられている。計算機1Dファイル1655のクリア・テキストは、暗号化操作1703に力入として供給される。この暗号化操作1703は、DES暗号化操作などの従来の暗号化操作であり、

ターゲット・コンピュータ1707の計算機1Dまたは修正済み計算機1Dなどの固有のターゲット・コンピュータ属性1705で鍵がかけられている。暗号化操作1699の出力は、製品キー(ソース・コンピュータ1651のキー・ファイル1653の一時製品キーと同じ)、顧客番号(ソース・コンピュータ1651のキー・ファイル1653の顧客番号と同じ)、クリア計算機1D(ターゲット・コンピュータ1707用の計算機1Dであって、ソース・コンピュータ1651の計算機1Dではない)、試用期間データ(ソース・コンピュータ1651のキー・ファイル1653の試用期間データと同じ)、およびソース・コンピュータ1651の計算機1DのIDを含む暗号化キー・ファイル1709を生成する。暗号化操作1703の出力は計算機1Dファイル1711を定義するもので、このファイルは、ターゲット・コンピュータ1707の計算機1D(ソース・コンピュータ1651の計算機1Dではない)と試用期間データ(ソース・コンピュータ1651の計算機1Dファイル1655の試用期間データと同じ)とを含む。

【0074】まとめとして、本発明の構成に関して以下の事項を開示する。

【0075】(1) 供給側であるソースからユーザにソフトウェア・オブジェクトを配布する方法において、永続暗号化キーを使用する暗号化操作で前記ソフトウェア・オブジェクトを暗号化するステップと、前記ソースから前記ユーザに前記暗号化ソフトウェア・オブジェクトを送るステップと、特定のシステム構成を有するユーザ制御のデータ処理システムに前記暗号化ソフトウェア・オブジェクトをロードするステップと、少なくとも一部が前記システム構成に基づく計算機1Dを導出するステップと、少なくとも一部が前記計算機1Dと前記永続暗号化キーとに基づく一時キーを導出するステップと、所定の期間、前記ユーザが前記一時キーを使用して前記永続暗号化キーを生成できるように、前記一時キーを受け取って、前記永続暗号化キーを生成するための永続キー生成機能を動作させ、前記ソフトウェア・オブジェクトへのアクセスを可能にするステップとを含む方法。

(2) 前記暗号化ソフトウェア・オブジェクトが、コンピュータがアクセス可能なメモリ媒体上に記録されて、前記ソースから前記ユーザに送られる、上記(1)に記載のソフトウェア・オブジェクトを配布する方法。

(3) 前記永続キー生成機能が、前記コンピュータがアクセス可能なメモリ媒体上に保持され、前記暗号化ソフトウェア・オブジェクトとともに前記ソースから前記ユーザに送られる、上記(2)に記載のソフトウェア・オブジェクトを配布する方法。

(4) 前記永続キー生成機能をその構成要素として含む、ファイル管理プログラムを、前記暗号化ソフトウェア・オブジェクトとともに前記ソースから前記ユーザに送るステップをさらに含む、上記(1)に記載のソフ

トウェア・オブジェクトを配布する方法。

(5) 少なくとも前記一時キーを記録するために前記ユーザ制御のデータ処理システム内にキー・ファイルを作成するステップを含む、上記(1)に記載のソフトウェア・オブジェクトを配布する方法。

(6) 少なくとも1つの固有のシステム属性を暗号化キーとして使用して、前記キー・ファイルを暗号化するステップを含む、上記(5)に記載のソフトウェア・オブジェクトを配布する方法。

(7) 作成者からユーザにソフトウェア・オブジェクトを配布する方法において、永続キーを使用して前記ソフトウェア・オブジェクトを暗号化するステップと、前記ソフトウェア・オブジェクトをコンピュータがアクセス可能なメモリ媒体にファイル管理プログラムとともに記録するステップと、前記作成者から前記ユーザに前記コンピュータがアクセス可能なメモリを送送するステップと、前記ファイル管理プログラムをユーザ制御のデータ処理システムにロードし、それを前記ユーザ制御のデータ処理システム用のオペレーティング・システムに関連付けるステップと、前記ファイル管理プログラムを使用して、前記ユーザ制御のデータ処理システムの少なくとも1つの属性に基づく計算機IDを導出するステップと、前記ユーザ制御のデータ処理システムで前記コンピュータがアクセス可能なメモリを読み取るステップと、少なくとも一部が前記計算機IDに基づく一時キーを導出するステップと、前記ユーザ制御のデータ処理システムで前記ファイル管理プログラムを実行することにより、前記一時キーによって定義される期間の間、前記ソフトウェア・オブジェクトへのアクセスを制限するステップと、前記ユーザ制御のデータ処理システムにおいて永続キー生成機能を実行することにより、少なくとも前記一時キーを受け取ったことに対する応答として前記永続キーを提供するステップとを含む方法。

(8) 前記ファイル管理プログラムが、前記ユーザ制御のデータ処理システムによって実行されるときに、複数の動作モードで動作可能であり、(a) 前記一時キーを使用することで前記ソフトウェア・オブジェクトが一時的に使用可能になる一時試動作モードと、(b) 前記ソフトウェア・オブジェクトを永続的に使用可能にして、前記ユーザによる前記ソフトウェア・オブジェクトの無制限使用を可能にする永続使用動作モードとを含むことを特徴とする、上記(7)に記載のソフトウェア・オブジェクトを配布する方法。

【0076】

【発明の効果】本発明のソフトウェア配布手法により、不正使用の問題を回避しつつ、ユーザに一次的な一定の試用期間を許容する機構が提供される。しかも、当該試用期間後もソフトウェア製品の使用を望むユーザについては、別途永続キーを付与することによりその目的が達成される。

【図面の簡単な説明】

【図1】ソフトウェア製品の試用期間使用を可能にする好ましい技法を実施する際に使用可能なスタンドアロン型データ処理システム、電話、およびコンピュータがアクセス可能な様々なメモリ媒体を示す絵画表現である。

【図2】ソフトウェア製品の試用期間使用を可能にする本発明の技法を使用可能な分散データ処理システムを示す絵画表現である。

【図3】本発明により計算機IDを生成するために使用可能なデータ処理システムの属性を示すブロック図である。

【図4】ソフトウェア・オブジェクトを暗号化するためのルーチンを示すブロック図である。

【図5】本発明の教示によりソース(ソフトウェア・ベンダ)とユーザ(顧客)との間で行われる情報交換を示す絵画表現である。

【図6】本発明によりユーザ・インタフェース・シェルを構築する際に使用される大まかなステップを示す流れ図である。

【図7】本発明によるベンダと顧客との対話を示す流れ図である。

【図8】本発明による試用期間操作を容易にするためのユーザ・インタフェース画面を示す図である。

【図9】本発明による試用期間操作を容易にするためのユーザ・インタフェース画面を示す図である。

【図10】本発明による試用期間操作を容易にするためのユーザ・インタフェース画面を示す図である。

【図11】本発明による試用期間操作を容易にするためのユーザ・インタフェース画面を示す図である。

【図12】一時アクセス・キーを開始するために使用されるユーザ・インタフェースを示す図である。

【図13】計算機IDを生成する好ましい技法を示すブロック図である。

【図14】本発明により計算機IDを暗号化するために使用される暗号化操作を示すブロック図である。

【図15】本発明により製品キーを生成する好ましい技法を示すブロック図である。

【図16】1つまたは複数のソフトウェア・オブジェクトの暗号解読に使用可能な実キーを生成するために一時製品キーを使用する好ましい技法を示すブロック図である。

【図17】図16のブロック図により導出された実キーの妥当性を検査する好ましい技法を示す図である。

【図18】図16のブロック図により導出された実キーの妥当性を検査する好ましい技法を示す図である。

【図19】一時製品キーを含む情報が入っているキー・ファイルを暗号化するための好ましいルーチンを示すブロック図である。

【図20】本発明により暗号化ファイル内の暗号化ヘッダを処理する好ましい技法を示すブロック図である。

【図 2 1】暗号化ソフトウェア・オブジェクトの暗号解読に使用可能な実キーを導出するためにユーザ制御のデータ処理システム内の複数の入力を使用する技法を示すブロック図である。

【図 2 2】図 2 1 により導出された実キーを使用する暗号解読操作を示す図である。

【図 2 3】実キーの妥当性を判定するために使用される比較操作を示すブロック図である。

【図 2 4】妥当性が検査された実キーを使用する暗号解読操作を示す図である。

【図 2 5】本発明による暗号化ヘッダの使い方を示す図である。

【図 2 6】本発明による暗号化ヘッダの使い方を示す図である。

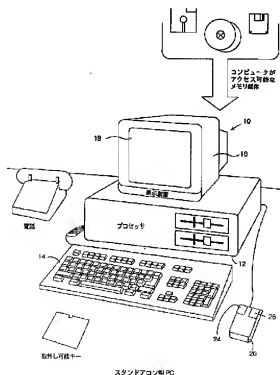
【図 2 7】本発明による暗号化ヘッダの使い方を示す図である。

【図 2 8】本発明による暗号化ヘッダの使い方を示す図である。

【図 2 9】本発明による暗号化ヘッダの使い方を示す図である。

【図 3 0】暗号化ソフトウェア・オブジェクトに関して試用期間使用を提供する好ましい技法を示す流れ図である。

【図 1】



【図 3 1】暗号化ソフトウェア・オブジェクトに関して試用期間使用を提供する好ましい技法を示す流れ図である。

【図 3 2】分散データ処理システム内で試用期間使用操作を実行するために使用可能なエクスポート操作を示す図である。

【図 3 3】分散データ処理システム内で試用期間使用操作を実行するために使用可能なインポート操作を示す図である。

【図 3 4】図 3 2 に示すエクスポート操作の代替図である。

【図 3 5】図 3 3 に示すインポート操作の代替図である。

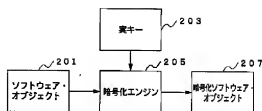
【図 3 6】エクスポート操作を実行するための代替技法を示すブロック図である。

【図 3 7】インポート操作を実行するための代替技法を示すブロック図である。

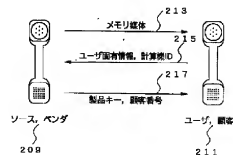
【符号の説明】

- 209 ソース、ベンダ
- 211 ユーザ、顧客
- 213 メモリ媒体
- 215 ユーザ固有情報、計算機 ID
- 217 製品キー、顧客番号

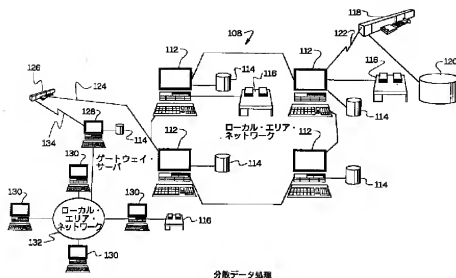
【図 4】



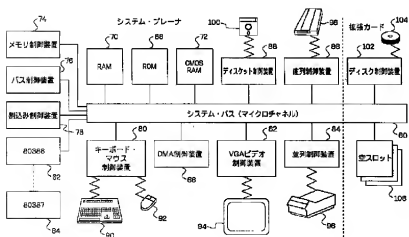
【図 5】



【図2】



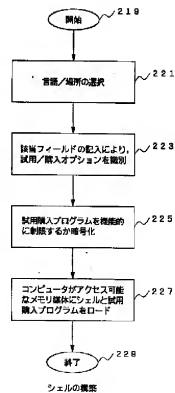
【図3】



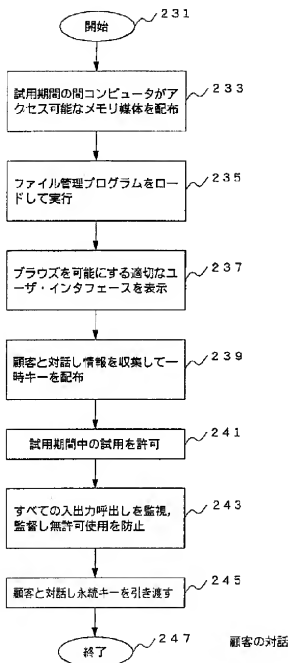
【図13】



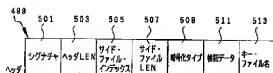
【図6】



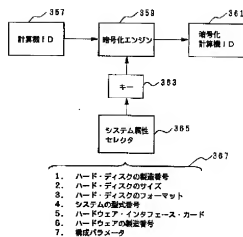
【図 7】



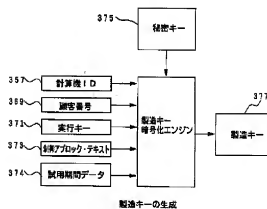
【図 27】



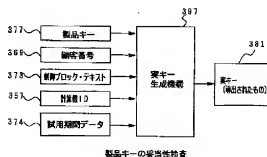
【図 14】



【図 15】



【図 16】



【図8】

Order Form

Order toll free + 24 hours a day + 7 days a week
1 - 800 - 724 - 9999

Node ID: 12345678 Machine ID: 9876543210 Customer ID: 0123-456-789

QTY	ITEM	DESCRIPTION	PRICE
	123456789012345	Lots 3-2-9 For Windows	\$48.05

SUBTOTAL: \$48.05

Payment methods: ☒ CREDIT CARD ☐ CHECK/MONEY ORDER ☐ NEW ORDER

Buttons: Close, Fax, Mail, Print, Unlock, Help

Don't sell, transfer, RESELL, RENT and RESALE and handling charges, if any, subject to change.

【図9】

Order Information

Address information: ☒ Customer address ☐ Ship to address (if different)

Name: Hillary Clinton

Address: 1800 Parson's Lane, Washington, D.C. 11112-5555

Phone: (410) 555-4992 ext. 6980

Fax: (410) 555-4300

Payment method: ☒ Visa ☐ MasterCard ☐ American Express ☐ Discover ☐ Other

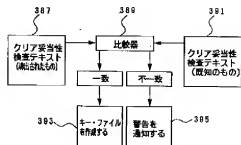
Payment information: Account number: 4438-3802-9387-3850 Expiration date: 5/95 VAT ID: 1234567890

Buttons: Print, Cancel

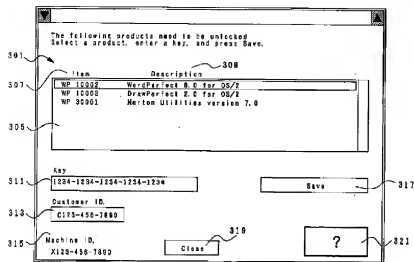
【図17】



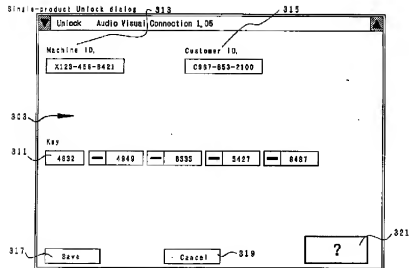
【図18】



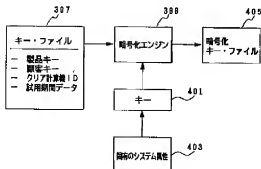
【図10】



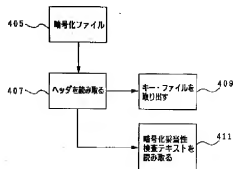
【図11】



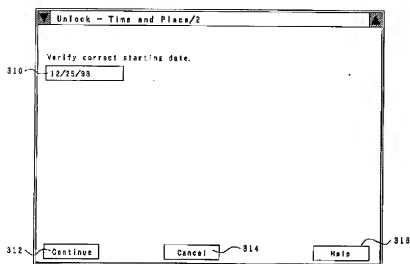
【図19】



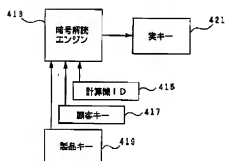
【図20】



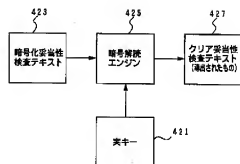
【図 12】



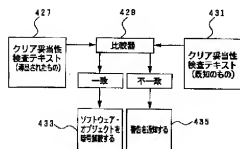
【図 21】



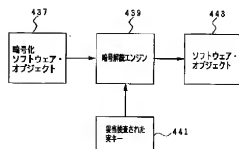
【図 22】



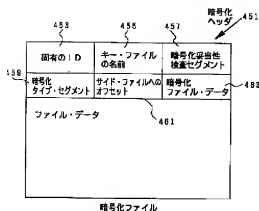
【図 23】



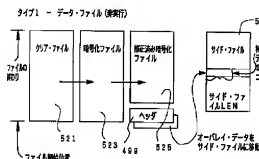
【図 24】



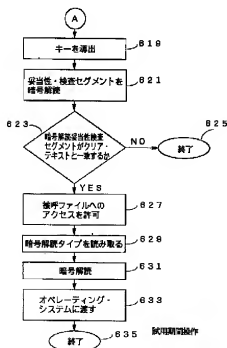
【図 25】



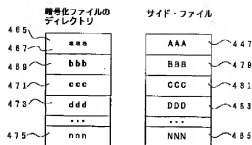
【図 28】



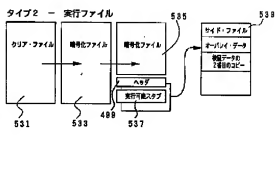
【図 31】



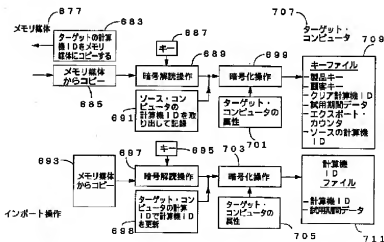
【図 26】



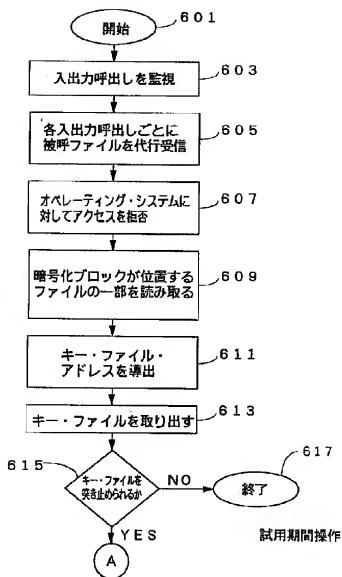
【図 29】



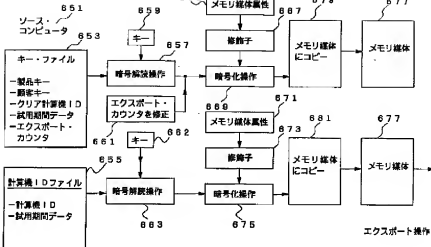
【図 33】



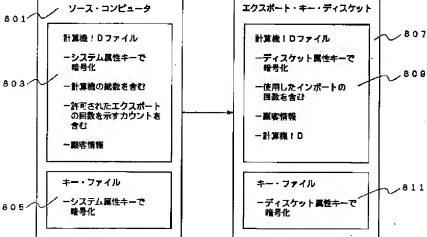
【図30】



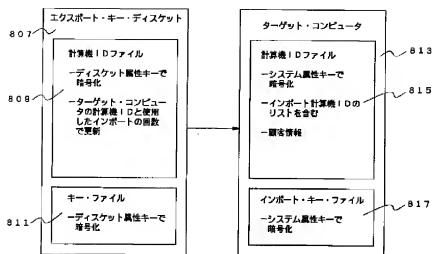
【图 3-2】



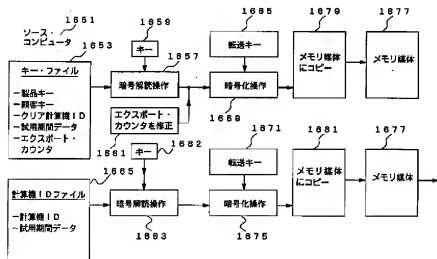
【图 3-4】



【图 3-6】



【图 3-6】



フロントページの続き

(72)発明者	ハドソン・ダブリュー・フィリップス アメリカ合衆国80301 コロラド州ボウル ダー ジェームストン・ストリート 4725	(72)発明者	ロバート・エフ・ブライアー アメリカ合衆国80503 コロラド州ロング モント マウント・ミーカー・ロード 7380
---------	---	---------	---

(72)発明者 ハドソン・ダブリュー・フィリップス
アメリカ合衆国80301 コロラド州ボウル
ダー ジェームストン・ストリート 4725

(72)発明者 ロバート・エフ・プライアー
アメリカ合衆国80503 コロラド州ロング
モント マウント・ミーカー・ロード
7380